PAT-NO: JP02003330897A

DOCUMENT-IDENTIFIER: JP 2003330897 A

TITLE: MULTI-CASTING RESTRICTED BY TIME FRAME FOR FUTURE DELIVERY MULTI-CASTING

PUBN-DATE: November 21, 2003

INVENTOR-INFORMATION:

NAME	COUNTRY
PADMANABHAN, VENKATA N	N/A
CABRERA, LUIS F	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
MICROSOFT CORP	N/A

APPL-NO: JP2003072636

APPL-DATE: March 17, 2003

PRIORITY-DATA: 2002099242 (March 15, 2002)

INT-CL (IPC): G06F015/00 , G06F013/00 , H04L009/08

ABSTRACT:

PROBLEM TO BE SOLVED: To transmit events in a specified time frame, as fairly as possible, to a variety of necessary number of clients.

SOLUTION: Before the release time of an event, the enciphered event is transmitted, and a key small in size and transmitted efficiently is distributed to decode the encipher of the event at the release time of the event or the other time so that clients can receive the event at a generally same time after the release time. Thus the event can be distributed to the clients with a variety of bandwidths.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－330897
（P2003－330897A）
(43)公開日　平成15年11月21日(2003.11.21)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
G06F	15/00	330	G06F	15/00	330Z　5B085
	13/00	540		13/00	540A　5J104
H04L	9/08		H04L	9/00	601C

審査請求　未請求　請求項の数68　ＯＬ　（全 24 頁）

(21)出願番号　特願2003－72636(P2003－72636)

(22)出願日　平成15年３月17日(2003.3.17)

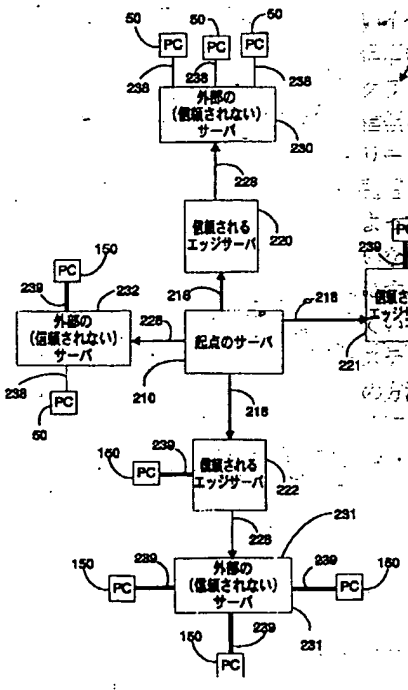
(31)優先権主張番号　１０／０９９，２４２
(32)優先日　平成14年３月15日(2002.3.15)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　391055933
マイクロソフト　コーポレイション
ＭＩＣＲＯＳＯＦＴ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国　ワシントン州　98052－6399　レッドモンド　ワン　マイクロソフト　ウェイ　（番地なし）
(74)代理人　100077481
弁理士　谷　義一　（外１名）

最終頁に続く

(54)【発明の名称】　フューチャデリバリマルチキャストのための時間窓によって制約されたマルチキャスト

(57)【要約】
【課題】　必要なだけの数の多様なクライアントにできる限り公正に所与の時間フレーム内でイベントを送信する。
【解決手段】　イベントのリリース時刻より前に暗号化したイベントを送信し、そのイベントをイベントのリリース時刻に、または別の時刻に暗号解読するための小さく効率的に伝送される鍵を配信して、各クライアントが、リリース時刻の後、ほぼ同時刻にイベントを受け取るようにすることにより、多様な帯域幅を有するクライアントにイベントを配信する。



1

【特許請求の範囲】

【請求項１】　所定のリリース時刻にリリースされることを意図する情報を有するイベントをネットワーク環境を介して少なくとも２つのクライアントに公正に配信するための方法であって、

前記リリース時刻より前に起点のサーバから少なくとも２つのクライアントに暗号化されたイベントを送信するステップ、および前記リリース時刻より後に鍵サーバから前記少なくとも２つのクライアントに暗号解読の鍵を送信するステップを含むことを特徴とする方法。

【請求項２】　前記暗号解読の鍵を送信するステップは、前記リリース時刻の直後に行われることを特徴とする請求項１に記載の方法。

【請求項３】　前記暗号解読の鍵を送信するステップは、前記少なくとも２つのクライアントのすべてが、前記暗号化されたイベントを受信するのを完了した後に行われることを特徴とする請求項１に記載の方法。

【請求項４】　前記イベントが、所定の終了時刻より前にリリースされることを意図し、また前記少なくとも２つのクライアントのすべてが、最終の鍵送信時刻より後に前記暗号化されたイベントの受信を完了する場合、前記少なくとも２つのクライアントのすべてが、前記暗号化されたイベントの受信を完了するのに先立って前記暗号解読の鍵を送信するステップが行われ、前記最終の鍵送信時刻は、前記少なくとも２つのクライアントのすべてへの前記鍵の伝送を可能にするのに十分なだけ前記終了時刻より前の時刻であることを特徴とする請求項１に記載の方法。

【請求項５】　前記リリース時刻より前に、前記基点のサーバから信頼されるエッジサーバに暗号化されていないイベントを送信するステップであって、そこでは前記信頼されるエッジサーバは、前記起点のサーバと接続のクライアントとの間の通信パス中のサーバであり、前記信頼されるエッジサーバは適切な時刻より前に情報をリリースすることがないと信頼されるステップ、および前記暗号解読の鍵が前記少なくとも２つのクライアントによって受信されるのとほぼ同時刻に、前記暗号化されていないイベントを第２のクライアントによって受信可能にする第２のクライアント送信時刻に、前記暗号化されていないイベントを前記第２のクライアントに送信するステップをさらに含むことを特徴とする請求項１に記載の方法。

【請求項６】　前記暗号解読の鍵が前記少なくとも２つのクライアントによって受信されるのとほぼ同時刻に、前記暗号化されていないイベントが第３のクライアントによって受信可能にする第３のクライアント送信時刻に、前記暗号化されていないイベントを前記第３のクライアントに送信するステップをさらに含むことを特徴とする請求項５に記載の方法。

【請求項７】　前記第２のクライアント送信時刻は、前記暗号化されていないイベントが、前記少なくとも２つのクライアントによって前記暗号解読の鍵が受信されるのとほぼ同時刻に、前記第２のクライアントまたは前記第３のクライアントのどちらか前記暗号化されていないイベントを先に受信すると予期される方によって受信可能となし、

前記第２のクライアント送信時刻に前記第３のクライアントに前記暗号化されていないイベントを送信するステップをさらに含むことを特徴とする請求項５に記載の方法。

【請求項８】　前記鍵サーバは、２つまたはそれより多[illegible]くの鍵サーバを含むことを特徴とする請求項１に記載の方法。

【請求項９】　前記暗号解読の鍵を送信するステップは、調整された鍵送信時刻に行われ、該鍵送信時刻は前記ネットワーク環境の中のすべてのクライアントが前記暗号化されたイベントをいつ受信するかに基づくことを特徴とする請求項１に記載の方法。

【請求項１０】　前記暗号解読の鍵を送信するステップは、前記暗号解読の鍵の少なくとも１つのコピーを含む鍵メッセージをマルチキャストするステップを含むことを特徴とする請求項１に記載の方法。

【請求項１１】　所定のリリース時刻にリリースされることを意図する情報を有するイベントをネットワーク環境を介して第１のクライアントに公正に配信するための暗号化されたイベント方法であって、

起点のサーバから、信頼されるエッジサーバに暗号化されたイベントを送信するステップであって、そこでは、前記信頼されるサーバは前記起点のサーバと接続のクライアントとの間の通信パス中のサーバであり、前記信頼されるエッジサーバは適切な時刻より前に情報をリリースすることがないと信頼されるステップ、

前記信頼されるエッジサーバにおいて前記暗号化されたイベントを暗号解読すること、および第１のクライアントに前記信頼されるエッジサーバから前記第１のクライアントに暗号解読されたイベントを送信するステップであって、前記第１のクライアント送信時刻は、前記暗号解読されたイベントの前記第１のクライアントへの第１の予期される伝送時間、および前記第１のクライアントが前記暗号解読されたイベントを受信する第１のクライアント着信時刻に相関し、前記第１のクライアント着信時刻は、前記リリース時刻より後であるステップを含むことを特徴とする方法。

【請求項１２】　前記第１の予期される伝送時間が、前記信頼されるエッジサーバと前記第１のクライアントの間の接続履歴を参照して判定されることを特徴とする請求項１１に記載の方法。

【請求項１３】　前記第１の予期される伝送時間が、前記信頼されるエッジサーバと前記第１のクライアントの間の第１のクライアント待ち時間をテストするネットワ

ーク機能の結果を参照して判定されることを特徴とする請求項１１に記載の方法。

【請求項１４】　前記第１のクライアント着信時刻は、前記リリース時刻であることを特徴とする請求項１１に記載の方法。

【請求項１５】　第２のクライアント送信時刻に前記信頼されるエッジサーバから第２のクライアントに前記暗号解読されたイベントを送信するステップであって、そこでは、前記第２のクライアント送信時刻は、前記第２のクライアントへの前記暗号解読されたイベントの第２の予期される伝送時間、および前記第２のクライアントが前記暗号解読されたイベントを受信する第２のクライアント着信時刻に相関し、前記第２のクライアント着信時刻は、前記リリース時刻より後であるステップをさらに含むことを特徴とする請求項１１に記載の方法。

【請求項１６】　前記第１のクライアント送信時刻は前記第２のクライアント送信時刻であることを特徴とする請求項１５に記載の方法。

【請求項１７】　前記第１のクライアント着信時刻は、前記第２のクライアント着信時刻であることを特徴とする請求項１５に記載の方法。

【請求項１８】　前記第１のクライアント着信時刻は、第２のクライアント鍵受信時刻とほぼ同一であり、

前記リリース時刻より前に前記起点のサーバから第２のクライアントに前記暗号化されたイベントを送信するステップ、および前記リリース時刻より後に鍵サーバから前記第２のクライアントに暗号解読の鍵を送信し、前記第２のクライアントは、前記第２のクライアント鍵受信時刻に前記暗号解読の鍵を受信するステップをさらに含むことを特徴とする請求項１１に記載の方法。

【請求項１９】　少なくとも２つのクライアントにネットワーク環境を介してイベントを公正に配信するための方法であって、

前記少なくとも２つのクライアントに暗号化されたイベントを送信するステップ、および前記少なくとも２つのクライアントのすべてが前記暗号化されたイベントを受信した後、前記少なくとも２つのクライアントに暗号解読の鍵を送信するステップを含むことを特徴とする方法。

【請求項２０】　信頼されるエッジサーバに暗号化されていないイベントを送信するステップであって、そこでは、信頼されるエッジサーバは前記ネットワーク環境の中のサーバであり、前記信頼されるエッジサーバは適切な時刻より前に情報をリリースすることがないと信頼されるステップ、および前記暗号解読の鍵が前記少なくとも２つのクライアントによって受信されるのとほぼ同時刻に、前記暗号化されていないイベントを第２のクライアントによって受信可能にする第２のクライアント送信時刻に、前記暗号化されていないイベントを前記第２のクライアントに送信するステップをさらに含むことを特

徴とする請求項１９に記載の方法。

【請求項２１】　信頼されるエッジサーバに暗号化されたイベントを送信するステップであって、そこでは、前記信頼されるエッジサーバは前記ネットワーク環境の中のサーバであり、前記信頼されるエッジサーバは適切な時刻より前に情報をリリースすることがないと信頼されるステップ、

前記信頼されるエッジサーバにおいて前記暗号化されたイベントを暗号解読するステップ、および第２のクライアント送信時刻に前記信頼されるエッジサーバから第２のクライアントに暗号解読されたイベントを送信するステップであって、そこでは、前記第２のクライアント送信時刻は、前記暗号解読されたイベントの前記第２のクライアントへの第２の予期される伝送時間、および前記第２のクライアントが前記暗号解読されたイベントを受信する第２のクライアント着信時刻に相関し、前記第２のクライアント着信時刻は、前記暗号解読の鍵が前記少なくとも２つのクライアントによって受信されるのとほぼ同時刻であるステップをさらに含むことを特徴とする請求項１９に記載の方法。

【請求項２２】　前記第２の予期される伝送時間が、前記信頼されるエッジサーバと前記第２のクライアントの間の接続履歴を参照して判定されることを特徴とする請求項２１に記載の方法。

【請求項２３】　前記第２の予期される伝送時間が、前記信頼されるエッジサーバと前記第２のクライアントの間の第２のクライアント待ち時間をテストするネットワーク機能の結果を参照して判定されることを特徴とする請求項２１に記載の方法。

【請求項２４】　所定のリリース時刻にリリースされることを意図する情報を有するイベントを少なくとも２つのクライアントにネットワーク環境を介して公正に配信するためのコンピュータ実行可能命令を有するコンピュータ可読媒体であって、

前記コンピュータ実行可能命令は、

前記リリース時刻より前に起点のサーバから前記少なくとも２つのクライアントに暗号化されたイベントを送信するステップ、および前記リリース時刻より後に鍵サーバから前記少なくとも２つのクライアントに暗号解読の鍵を送信するステップを実行することを特徴とするコンピュータ可読媒体。

【請求項２５】　前記暗号解読の鍵を送信するステップは、前記少なくとも２つのクライアントが前記暗号化されたイベントの受信を完了した後に行われることを特徴とする請求項２４に記載のコンピュータ可読媒体。

【請求項２６】　前記コンピュータ実行可能命令は、

前記リリース時刻より前に前記起点のサーバから、信頼されるエッジサーバに暗号化されていないイベントを送信するステップであって、そこでは、前記信頼されるエッジサーバは前記起点のサーバと、接続のクライアント

5

との間の通信パス中のサーバであり、前記信頼されるエッジサーバは適切な時刻より前に情報をリリースすることがないと信頼されるステップ、および前記暗号解読の鍵が前記少なくとも２つのクライアントによって受信されるのとほぼ同時刻に、前記暗号化されていないイベントが第２のクライアントによって受信可能にする第２のクライアント送信時刻に、前記暗号化されていないイベントを前記第２のクライアントに送信するステップをさらに実行することを特徴とする請求項２４に記載のコンピュータ可読媒体。

【請求項２７】　前記コンピュータ実行可能命令は、前記暗号解読の鍵が前記少なくとも２つのクライアントによって受信されるのとほぼ同時刻に、前記暗号化されていないイベントが第３のクライアントによって受信可能にする第３のクライアント送信時刻に、前記暗号化されていないイベントを前記第３のクライアントに送信するステップをさらに実行することを特徴とする請求項２６に記載のコンピュータ可読媒体。

【請求項２８】　前記第２のクライアント送信時刻は、前記暗号化されていないイベントが、前記少なくとも２つのクライアントによって前記暗号解読の鍵が受信されるのとほぼ同時刻に、前記第２のクライアントまたは前記第３のクライアントのどちらか前記暗号化されていないイベントを先に受信すると予期される方によって受信可能となし、

前記コンピュータ実行可能命令は、

前記第２のクライアント送信時刻に前記第３のクライアントに前記暗号化されていないイベントを送信するステップをさらに実行することを特徴とする請求項２６に記載のコンピュータ可読媒体。

【請求項２９】　前記鍵サーバは、２つまたはそれより多くの鍵サーバを含むことを特徴とする請求項２４に記載のコンピュータ可読媒体。

【請求項３０】　前記暗号解読の鍵を送信するステップは、調整された鍵送信時刻に行われ、前記鍵送信時刻は前記ネットワーク環境の中のすべてのクライアントが前記暗号化されたイベントをいつ受信するかに基づくことを特徴とする請求項２４に記載のコンピュータ可読媒体。

【請求項３１】　所定のリリース時刻にリリースされることを意図する情報を有するイベントを第１のクライアントにネットワーク環境を介して公正に配信するためのコンピュータ実行可能命令を有するコンピュータ可読媒体であって、

前記コンピュータ実行可能命令は、

起点のサーバから、信頼されるエッジサーバに暗号化されたイベントを送信するステップであって、そこでは、前記信頼されるエッジサーバは前記起点のサーバと、接続のクライアントの間との通信パス中のサーバであり、前記信頼されるエッジサーバは適切な時刻より前に情報

6

をリリースすることがないと信頼されるステップ、

前記信頼されるエッジサーバにおいて前記暗号化されたイベントを暗号解読するステップ、および第１のクライアント送信時刻に前記信頼されるエッジサーバから前記第１のクライアントに暗号解読されたイベントを送信するステップであって、そこでは、前記第１のクライアント送信時刻は、前記暗号解読されたイベントの前記第１のクライアントへの第１の予期される伝送時間、および前記第１のクライアントが前記暗号解読されたイベントを受信する第１のクライアント着信時刻に相関し、前記第１のクライアント着信時刻は、前記リリース時刻より後であるステップを実行することを特徴とするコンピュータ可読媒体。

【請求項３２】　前記第１の予期される伝送時間が、前記信頼されるエッジサーバと前記第１のクライアントの間の接続履歴を参照して判定されることを特徴とする請求項３１に記載のコンピュータ可読媒体。

【請求項３３】　前記第１の予期される伝送時間が、前記信頼されるエッジサーバと前記第１のクライアントの間の第１のクライアント待ち時間をテストするネットワーク機能の結果を参照して判定されることを特徴とする請求項３１に記載のコンピュータ可読媒体。

【請求項３４】　前記コンピュータ実行可能命令は、第２のクライアント送信時刻に前記信頼されるエッジサーバから第２のクライアントに前記暗号解読されたイベントを送信するステップであって、そこでは、前記第２のクライアント送信時刻は、前記第２のクライアントへの前記暗号解読されたイベントの第２の予期される伝送時間、および前記第２のクライアントが前記暗号解読されたイベントを受信する第２のクライアント着信時刻に相関し、前記第２のクライアント着信時刻は、前記リリース時刻より後であるステップをさらに実行することを特徴とする請求項３１に記載のコンピュータ可読媒体。

【請求項３５】　前記第１のクライアント送信時刻は、前記第２のクライアント送信時刻であることを特徴とする請求項３４に記載のコンピュータ可読媒体。

【請求項３６】　前記第１のクライアント着信時刻は、前記第２のクライアント着信時刻であることを特徴とする請求項３４に記載のコンピュータ可読媒体。

【請求項３７】　前記第１のクライアント着信時刻は、第２のクライアント鍵受信時刻とほぼ同一であり、

前記コンピュータ実行可能命令は、前記リリース時刻より前に前記起点のサーバから第２のクライアントに前記暗号化されたイベントを送信するステップ、および前記リリース時刻より後に鍵サーバから前記第２のクライアントに暗号解読の鍵を送信ステップであって、前記第２のクライアントは前記第２のクライアント鍵受信時刻に前記暗号解読の鍵を受信するステップを実行することを特徴とする請求項３１に記載のコンピュータ可読媒体。

【請求項３８】　イベントを少なくとも２つのクライアントにネットワーク環境を介して公正に配信するためのコンピュータ実行可能命令を有するコンピュータ可読媒体であって、
前記コンピュータ実行可能命令は、
前記少なくとも２つのクライアントに暗号化されたイベントを送信するステップ、および前記少なくとも２つのクライアントのすべてが前記暗号化されたイベントを受信した後、前記少なくとも２つのクライアントに暗号解読の鍵を送信するステップを実行することを特徴とするコンピュータ可読媒体。
【請求項３９】　前記コンピュータ実行可能命令は、
信頼されるエッジサーバに暗号化されたイベントを送信するステップであって、そこでは、前記信頼されるエッジサーバは前記ネットワーク環境の中のサーバであり、前記信頼されるエッジサーバは適切な時刻より前に情報をリリースすることがないと信頼されるステップ、
前記信頼されるエッジサーバにおいて前記暗号化されたイベントを暗号解読するステップ、および第２のクライアント送信時刻に前記信頼されるエッジサーバから第２のクライアントに暗号解読されたイベントを送信するステップであって、そこでは、前記第２のクライアント送信時刻は、前記暗号解読されたイベントの前記第２のクライアントへの第２の予期される伝送時間、および前記第２のクライアントが前記暗号解読されたイベントを受信する第２のクライアント着信時刻に相関し、前記第２のクライアント着信時刻は、前記暗号解読の鍵が前記少なくとも２つのクライアントによって受信されるのとほぼ同時刻であるステップを実行することを特徴とする請求項３８に記載のコンピュータ可読媒体。
【請求項４０】　所定のリリース時刻にリリースされることを意図する情報を有するイベントを公正に配信するためのシステムであって、
起点のサーバと、
適切な時刻より前に情報をリリースすることがないと信頼され、前記起点のサーバと、接続されたクライアントとの間の通信パス中のサーバである、信頼されるエッジサーバと、
鍵サーバと、
少なくとも２つのクライアントとを含み、
前記起点のサーバは、前記リリース時刻より前に前記少なくとも２つのクライアントに暗号化されたイベントを送信し、また前記鍵サーバは、前記リリース時刻より後に前記少なくとも２つのクライアントに暗号解読の鍵を送信することを特徴とするシステム。
【請求項４１】　前記鍵サーバは、前記少なくとも２つのクライアントのすべてが前記暗号化されたイベントを受信するのを完了した後に前記暗号解読の鍵を送信することを特徴とする請求項４０に記載のシステム。
【請求項４２】　第２のクライアントをさらに含み、前記起点のサーバは、前記信頼されるエッジサーバに暗号化されていないイベントを送信し、また前記信頼されるエッジサーバは、前記暗号解読の鍵が前記少なくとも２つのクライアントによって受信されるのとほぼ同時刻に、前記暗号化されていないイベントが前記第２のクライアントによって受信されるのを可能にする第２のクライアント送信時刻に、前記暗号化されていないイベントを前記第２のクライアントに送信することを特徴とする請求項４０に記載のシステム。
【請求項４３】　前記少なくとも２つのクライアントに前記暗号化されたイベントを送信する前記起点のサーバは、前記信頼されるエッジサーバに暗号解読されていないイベントを送信する起点のサーバ、前記暗号化されクライアントに送信ていないイベントを暗号化する、信頼されるエッジサーバは前記第１のクライアント、および前記暗号化されたイベントを前記少なくとも２つのクライアントに送信する、信頼されるエッジサーバを含むことを特徴とする請求項４０に記載のシステム。
【請求項４４】　前記鍵サーバは調整された鍵送信時刻に前記暗号解読の鍵を送信し、前記調整された鍵送信時刻は前記少なくとも２つのクライアントが前記暗号化されたイベントをいつ受信するかに基づくことを特徴とする請求項４０に記載のシステム。
【請求項４５】　第２のクライアントをさらに含み、前記起点のサーバは前記信頼されるエッジサーバに前記暗号化されたイベントを送信し、前記鍵サーバは前記信頼されるエッジサーバに前記暗号解読の鍵を送信し、前記信頼されるエッジサーバは、前記暗号化されたイベントを暗号解読し、前記信頼されるエッジサーバは、前記暗号解読の鍵が前記少なくとも２つのクライアントによって受信されるのとほぼ同時刻に、前記暗号解読されたイベントが前記第２のクライアントによって受信可能にする第２のクライアント送信時刻に、前記暗号解読されたイベントを前記第２のクライアントに送信することを特徴とする請求項４０に記載のシステム。
【請求項４６】　前記鍵サーバは、前記暗号解読の鍵の少なくとも１つのコピーを含む鍵メッセージをマルチキャストすることを特徴とする請求項４０に記載のシステム。
【請求項４７】　所定のリリース時刻にリリースされることを意図する情報を有するイベントを公正に配信するためのシステムであって、
起点のサーバと、
適切な時刻より前に情報をリリースすることがないものと信頼することができる、前記起点のサーバと接続されたクライアントの間の通信パス中のサーバである、信頼されるエッジサーバと、
第１のクライアントとを含み、
前記信頼されるエッジサーバは、第１のクライアント送信時刻に前記第１のクライアントに暗号化されていない

イベントを送信し、前記第１のクライアント送信時刻は、前記暗号解読されたイベントの前記第１のクライアントへの第１の予期される伝送時間、および前記第１のクライアントが前記暗号解読されたイベントを受信する第１のクライアント着信時刻に相関し、前記第１のクライアント着信時刻は、前記リリース時刻より後であることを特徴とするシステム。

【請求項４８】　第２のクライアントをさらに含み、前記起点のサーバは、前記信頼されるエッジサーバに暗号化されたイベントを送信し、前記信頼されるエッジサーバは、前記暗号化されたイベントを暗号解読し、また前記信頼されるエッジサーバは、前記暗号解読されたイベントを前記第２のクライアントに送信して、前記第２のクライアントが、ほぼ前記第１のクライアント着信時刻に前記暗号解読されたイベントを受信するようにすることを特徴とする請求項４７に記載のシステム。

【請求項４９】　前記第１の予期される伝送時間が、前記信頼されるエッジサーバと前記第１のクライアントの間の接続履歴を参照して判定されることを特徴とする請求項４７に記載のシステム。

【請求項５０】　前記第１の予期される伝送時間が、前記信頼されるエッジサーバと前記第１のクライアントの間の第１のクライアント待ち時間をテストするネットワーク機能の結果を参照して判定されることを特徴とする請求項４７に記載のシステム。

【請求項５１】　第２のクライアント送信時刻に前記信頼されるエッジサーバから第２のクライアントに前記暗号化されていないイベントを送信し、前記第２のクライアント送信時刻は、前記第２のクライアントへの前記暗号化されていないイベントの第２の予期される伝送時間、および前記第２のクライアントが前記暗号化されていないイベントを受信する第２のクライアント着信時刻に相関し、前記第２のクライアント着信時刻は、前記リリース時刻より後であることを特徴とする請求項４７に記載のシステム。

【請求項５２】　前記第１のクライアント送信時刻は、前記第２のクライアント送信時刻であることを特徴とする請求項５１に記載のシステム。

【請求項５３】　前記第１のクライアント着信時刻は、前記第２のクライアント着信時刻であることを特徴とする請求項５１に記載のシステム。

【請求項５４】　鍵サーバをさらに含み、前記起点のサーバは、前記リリース時刻より前に第２のクライアントに暗号化されたイベントを送信し、また前記鍵サーバは、前記リリース時刻より後に前記第２のクライアントに暗号解読の鍵を送信し、前記第２のクライアントは、前記第１のクライアント着信時刻に前記暗号解読の鍵を受信することを特徴とする請求項４７に記載のシステム。

【請求項５５】　イベントを公正に配信するためのシステムであって、
サーバと、
少なくとも２つのクライアントとを含み、前記サーバは、前記少なくとも２つのクライアントに暗号化されたイベントを送信し、また前記サーバは、前記少なくとも２つのクライアントのすべてが前記暗号化されたイベントを受信した後に前記少なくとも２つのクライアントに暗号解読の鍵を送信することを特徴とするシステム。

【請求項５６】　第２のクライアントをさらに含み、前記サーバは、適切な時刻より前に情報をリリースすることがないものと信頼することができるサーバである信頼されるエッジサーバであり、前記信頼されるエッジサーバは、前記暗号解読の鍵が前記少なくとも２つのクライアントによって受信されるのとほぼ同時刻に、前記暗号化されていないイベントが前記第２のクライアントによって受信可能にする第２のクライアント送信時刻に、暗号化されていないイベントを前記第２のクライアントに送信することを特徴とする請求項５５に記載のシステム。

【請求項５７】　第２のクライアントをさらに含み、前記サーバは、適切な時刻より前に情報をリリースすることがないものと信頼することができるサーバである信頼されるエッジサーバであり、またさらに前記信頼されるエッジサーバであって、エッジサーバは、暗号化されたイベントを受信し、前記暗号化されたイベントを暗号解読し、前記暗号解読の鍵が前記少なくとも２つのクライアントによって受信されるのとほぼ同時刻に、前記暗号解読されたイベントが前記第２のクライアントによって受信されるのを可能にする第２のクライアント送信時刻に、前記暗号解読されたイベントを前記第２のクライアントに送信することを特徴とする請求項５５に記載のシステム。

【請求項５８】　前記第２のクライアント送信時刻が、前記信頼されるエッジサーバと前記第２のクライアントの間の接続履歴を参照して判定されることを特徴とする請求項５７に記載のシステム。

【請求項５９】　前記第２のクライアント送信時刻が、前記信頼されるエッジサーバと前記第２のクライアントの間の第２のクライアント待ち時間をテストするネットワーク機能の結果を参照して判定されることを特徴とする請求項５７に記載のシステム。

【請求項６０】　所定のリリース時刻にリリースされることを意図する情報を有するイベントをネットワーク環境を介して少なくとも２つのクライアントに公正に配信するための方法であって、
前記リリース時刻より前に起点のサーバから前記少なくとも２つのクライアントに暗号化されたイベントを送信するステップと、
前記リリース時刻より後に鍵サーバから前記少なくとも２つのクライアントに暗号解読の鍵を送信するステップとを含むことを特徴とする方法。

【請求項６１】　前記暗号解読の鍵を前記送信するステップは、前記少なくとも２つのクライアントのすべてが前記暗号化されたイベントを受信した後に行われることを特徴とする請求項６０に記載の方法。

【請求項６２】　前記リリース時刻より前に前記起点のサーバから信頼されるエッジサーバに暗号化されていないイベントを送信するステップであって、そこでは、前記信頼されるエッジサーバは前記起点のサーバと、接続されたクライアントとの間の通信パス中のサーバであり、前記信頼されるエッジサーバは、適切な時刻より前に情報をリリースすることがないと信頼されるステップと、

前記暗号解読の鍵が前記少なくとも２つのクライアントによって受信されるのとほぼ同時刻に、前記暗号化されていないイベントが第２のクライアントによって受信可能にする第２のクライアント送信時刻に、前記暗号化されていないイベントを前記第２のクライアントに送信するステップとをさらに含むことを特徴とする請求項６０に記載の方法。

【請求項６３】　適切な時刻より前に情報をリリースすることがないと信頼することができ、前記起点のサーバと、接続されたクライアントの間の通信パス中のサーバである、信頼されるエッジサーバであって、

リリース時刻より前に、前記リリース時刻にリリースされることを意図する情報を有する暗号化されたイベントを前記第１のクライアントに送信するための手段と、

前記リリース時刻より後に前記第１のクライアントに暗号解読の鍵を送信するための手段とを含むことを特徴とするサーバ。

【請求項６４】　前記暗号解読の鍵の送信は、前記第１のクライアントが前記暗号化されたイベントを受信するのを完了した後に行われることを特徴とする請求項６３に記載の信頼されるエッジサーバ。

【請求項６５】　前記暗号化されたイベントを暗号解読するための手段と、

前記暗号解読の鍵が前記第１のクライアントによって受信されるのとほぼ同時刻に、前記暗号解読されたイベントが第２のクライアントによって受信可能にする第２のクライアント送信時刻に、前記暗号解読されたイベントを前記第２のクライアントに送信するための手段とをさらに含むことを特徴とする請求項６３に記載の信頼されるエッジサーバ。

【請求項６６】　前記第２のクライアント送信時刻が、前記信頼されるエッジサーバと前記第２のクライアントの間の接続履歴を参照して判定されることを特徴とする請求項６５に記載の信頼されるエッジサーバ。

【請求項６７】　前記第２のクライアント送信時刻が、前記信頼されるエッジサーバと前記第２のクライアントの間の第２のクライアント待ち時間をテストするネットワーク機能の結果を参照して判定されることを特徴とする請求項６５に記載の信頼されるエッジサーバ。

【請求項６８】　前記暗号解読の鍵が前記第１のクライアントによって受信されるのとほぼ同時刻に、前記暗号化されていないイベントが第２のクライアントによって受信されるのを可能にする第２のクライアント送信時刻に、前記暗号化されていないイベントを前記第２のクライアントに送信するための手段をさらに含むことを特徴とする請求項６３に記載の信頼されるエッジサーバ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、一般にネットワークを介するコンテンツ配信に関し、より詳細には、所与の時間フレーム内に複数のクライアントにコンテンツなどのアナログ接続を配信することに関する。

【０００２】

【従来の技術】ここ３０年間でインターネットは、政府およびいくつかの教育機関によって管理されるいくつかのサーバから、サーバおよびクライアントの巨大な多様なネットワークに成長した。インターネット上のサーバは、自動車の広告や販売から古代ギリシア語の手稿に至るまでを範囲に含む、かつてないほど多くのことを提供している。インターネットの範囲および影響力は、次の少なくとも３つの相互関連する要因により着実に成長している。すなわち、ますます増大するコンピュータ能力、ますます増加する帯域幅、およびますます多くのユーザの要求とともに一般に成長する一方で、増加するユーザ数である。残念ながら、計算能力がユーザ数の急激な増加に追い越される可能性があり、またときどきで追い越されている。

【０００３】この問題は、より小さいインターネットおよびローカルエリアネットワークにおいて顕著である可能性があるが、インターネットではより大きくなる。例えば、政府または裁判所の告知または新しい音楽ビデオのクリップなどの重要なニュースまたはエンターテインメントのリリースにより、リリースを行うＷｅｂサイトに毎分数百万のヒットがもたらされる可能性がある。この問題は、効率的なサービスプロバイダおよびＷｅｂサーバの帯域幅が必然的に有限であるため、そのような大量の要求によってサイトが圧倒される可能性があり、また通常、数秒間かかるダウンロードに、数分間、またさらには数時間もかかる可能性がある。ユーザの接続速度が向上しまたユーザがより高速のダウンロードに慣れてくるにつれ、サービスのこの遅延は、ますます重要性を帯びている。

【０００４】この問題の解決策の１つは、マルチキャスティングである。マルチキャスティングは、データの１つのストリームだけを送信するサーバによって同時に多数の異なるユーザにストリーミングコンテンツを送信するのを可能にするインターネットプロトコルである。次のとおり、特定のポートがマルチキャスティングのため

に使用される。サーバが、ストリーミングデータをこのポートに送信し、マルチキャストを受信するのを望むクライアントが、その指定されたポートを「聴取」する。この方法を使用して、通常の「ユニキャスティング」の帯域幅問題のいくつかを克服することができ、またユーザは、より適時にデータを受け取ることができる。残念ながら、このより効率的な方法でさえ、多数のユーザが、マルチキャストを聴取しようと試みている場合、圧倒される可能性がある。さらに、多様な接続速度のユーザが、マルチキャスティングプロトコルを同等に活用することは困難である。ダイヤル呼出しのインターネットサービスプロバイダ（ＩＳＰ）を介するなどしてインターネットへの一般的なアナログ接続を有するユーザは、常に、ケーブルモデムまたはデジタル加入者回線（ＤＳＬ）モデムなどのブロードバンドインターネット接続を有するユーザの後でデータを受け取る。

【０００５】インターネットによって配信される一部の情報は、多数のユーザができる限り迅速にコンテンツをダウンロードするのが重要なだけでなく、ユーザが、コンテンツを同時刻に受け取る、または指定された時間量の範囲内で受け取ることも重要であることで、さらなる厄介な問題を有する。情報の受取りのタイミングが重要である可能性がある状況の一例は、金融市場に影響を与える可能性がある政府データのリリースである。そのような状況では、情報を最初に受け取る人々が、その情報をまだ受け取っていない人々から利益を得る立場にある。別の例は、人気のある音楽家または音楽グループからの音楽ビデオクリップのリリースであることが可能である。この例は、そのようなリリースが、多数のメガバイトのサイズである可能性があり、配信が困難になるというさらなる問題を有する。さらに、一般に、政府データまたは音楽ビデオクリップが最初にリリースされる最初の時刻が存在する。したがって、問題は、どのようにして、このリリースの時刻にできる限り近く、ただし、その情報が無用または陳腐になる何らかの後の時点の後ではなく、グループのクライアントにイベントを送るかということになる。この問題は、効率と公正さの両方の点で意味がある。

【０００６】このタスクを達成する際の１つの困難は、前述したネットワーク帯域幅の問題である。ほとんどの企業ネットワークは、現在、高速バックボーンでインターネットに接続されているが、アナログモデムを使用してインターネットに接続する多数のユーザが、まだ存在する。ＤＳＬ接続などのブロードバンド接続を介してインターネットに接続されるユーザが、５６Ｋｂｐｓのダイヤル呼出し接続を介して接続されるユーザと同時刻に情報にアクセスするのを開始できたとすると、ブロードバンド接続を有するユーザは、遅い方の接続上のユーザよりはるかに前にその情報を受け取るのを終えることになる。例えば、ダウンロードされるイベントのサイズ

が、１０ＭＢであったとすると、５６Ｋｂｐｓの接続では、そのイベントをダウンロードするにはおよそ２４分間かかり、１Ｍｂｐｓのデジタル加入者回線では、８０秒間だけかかる。

【０００７】

【発明が解決しようとする課題】コンテンツ配信の現在の方法は、必要なだけの数の多様なクライアントにできる限り公正に所与の時間フレーム内でイベントを送信することを容易にするツールをほとんど提供していない。コンテンツプロバイダおよびサービスプロバイダは、一般に、配信の公正さ、または特定の時刻におけるアクセスに全く注意を払わない。したがって、最も高速のもっとも恵まれたユーザが、早い時刻にコンテンツを受け取ることができり、しばしば、そのようなユーザが、他のユーザよりさらに公正さを提供しようとわち、ネットワーク帯域幅および自らの接続速度に比例して後の時刻にその情報を受け取る他のユーザから不当に利益を得ることを許している。

【０００８】本発明は、イベントのリリース時刻より前に暗号化したイベントを送信し、そのイベントをイベントのリリース時刻に、または別の時刻に暗号解読するための小さく効率的に伝送される鍵を配信して、各クライアントが、リリース時刻の後、ほぼ同時刻にイベントをそのコンテンツを受け取るようにすることにより、多様な帯域幅を有するクライアントにイベントを配信するための方法、コンピュータ可読媒体、およびシステムを目的とする。

【０００９】本発明は、１つまたは複数のクライアントに接続された信頼されるサーバに、イベントのリリース時刻より前に暗号化されたイベントを送信し、イベントのリリース時刻に、またはより早期にそのイベントを暗号解読する鍵を配信し、サーバにおいてイベントを暗号解読し、イベントのリリース時刻または別の時刻に、接続されたクライアントにサーバからそのイベントを配信し、各クライアントが、リリース時刻の後、ほぼ同時刻にイベントを受け取ることにより、多様な帯域幅を有するクライアントにイベントを配信するための方法、コンピュータ可読媒体、およびシステムをさらに目的とする。

【００１０】また、本発明は、イベントのリリース時刻に先立つか、またはリリース時刻に暗号化されたイベントまたはサートを送信し、また時間フレームの終了、すなわち、その時点を過ぎるとイベントが、もはや有用ではなくなる時間フレームの終了、またはもはや有意義ではない時間フレームの終了に十分に先立つ時刻にイベントを暗号解読するための小さく効率的に伝送される鍵を送信することにより、コンテンツ配信の公正さを確実にするための方法、コンピュータ可読媒体、およびシステムも目的とする。

【００１１】さらに、本発明は、複数のユニキャストコピーまたはマルチキャストコピーを介して小さく効率的に伝送される鍵を送信する方法、コンピュータ可読媒

体、およびシステムを対象とする。そのようなコピーは、単一の信頼されるサーバにより、鍵を送信することに専用の特殊化されたサーバにより、または複数の信頼されるサーバによって同時刻に送信することができる。異なるサーバからなど、複数のネットワークパスを介して鍵を送信することにより、鍵の少なくとも1つのコピーが、適切な時刻に各クライアントによって受け取られる可能性が大幅に高くなる。

【0012】

【課題を解決するための手段】本発明は、関心を有するクライアントが、クライアントの接続帯域幅の違いにも関わらず、所与のリリース時刻にリリースされたイベントをほぼ同時刻に受け取ることができるようにすることにより、配信の公正さを提供しようと試みるメカニズムを企図している。接続帯域幅の違いは、クライアントがサーバに接続されている速度、サーバ間接続の輻輳等を含め、いくつかの要因に起因する可能性がある。少なくとも1つの起点のサーバが、リリースされるべきデータを含む。起点のサーバは、いくつかの信頼されるエッジサーバに接続されていることが可能であり、信頼されるエッジサーバは、自らに接続された信頼されないサーバおよびクライアントにコンテンツをさらに配信する。替わりに、起点のサーバは、信頼されないサーバまたはクライアントに直接に接続することが可能である。信頼されるエッジサーバは、選択されたリリース時刻の前に情報をリリースしないものと信頼することができるサーバである。したがって、信頼されるエッジサーバは、信頼されるサーバ、少なくとも1つの起点のサーバ、および信頼されるサーバと起点のサーバの間の接続を含む配信ネットワークの「エッジ」に存在する。

【0013】データがクライアントにリリースされる時刻より前に、1つまたは複数の起点のサーバからクライアントに暗号化されたデータを配信することができ、クライアントは、そのデータをローカルで記憶し、暗号解読する。その後、リリース時刻に、またはリリース時刻の後、暗号化されたデータを暗号解読することができる小さく効率的に伝送される鍵をクライアントに送信することができる。鍵は、一般に、十分に小さいサイズのものであるため、クライアントまたはサーバのそれぞれが、狭い時間範囲内でその鍵を受け取ることができ、各クライアントが、ほぼ同時刻にデータへのアクセスを得るのが確実になるはずである。

【0014】また、暗号化されたデータをサーバにおいて暗号解読してから、暗号化されていない形態でクライアントに送信することもできる。暗号解読を行うサーバが、信頼されるエッジサーバである場合、暗号化されたデータおよび鍵は、リリース時刻より前に送信することができる。信頼されるエッジサーバは、そのデータを暗号解読し、リリース時刻に、またはリリース時刻より前にそのデータをクライアントに送信して、クライアントがリリース時刻にデータを受け取るようにすることができる。あるいは、サーバが、信頼されるエッジサーバではない場合、データをやはりリリース時刻より前に送信するが、鍵はリリース時刻に送信し、できる限り迅速に、または調整された時刻にデータを暗号解読してクライアントに送信することが可能である。

【0015】また、本発明は、暗号化されたデータをリリース時刻に、またはリリース時刻の後にクライアントに送信することができるが、鍵は、各クライアントが、ほぼ同時に鍵を受け取るような時刻まで、またはデータが配布される時間窓が満了するより前にできる限り多数のクライアントが鍵を受け取るような時刻まで伝送されないようにすることも企図される。暗号化されたデータがリリースされるべきを、時間窓の満了より前にクライアントのすべての伝送の待ち行列を空送が完了しているように送信することが可能な場合、鍵時刻に開始することの伝送は、各クライアントが暗号化されたデータを受け取るまで遅延させることができる。替わりに、時間窓の満了より前に各クライアントに暗号化されたデータを配信することができない場合、鍵は、各クライアントへの暗号化されたデータの配信の完了より幾分前の時間に送信することができる。同様に、配信要件が、情報を公正に配布するよりも、迅速に配布することの方が重要であり、および一部のクライアントを同じサーバに、各クライアントが暗号化されたデータを受け取る前に鍵をより効果的に送信することができる。

【0016】さらに、本発明は、起点のサーバまたは信頼されるエッジサーバにかかる伝送の負担を最小限に抑えるマルチキャスティングプロトコルの使用を企図している。マルチキャスティングプロトコルを使用することにより、サーバは、いくつかのコピーを送信するだけでよく、次に、そのコピーが、ルータによって複製されてさらなるサーバまたはクライアントに転送される。マルチキャスティングプロトコルの特に適切な用法が、鍵の伝送であり得る。鍵は、非常に少量のデータである可能性があるため、クライアントからの再送要求を待つのではなく、鍵の冗長なコピーをマルチキャストすることにより、効率の向上を実現することができる。また、鍵は、クライアントが大量の冗長性を使用する誤り訂正とともにマルチキャストするのではなく、単にその鍵をマルチキャストして、再送要求を回避することもできる。さらに、複数のサーバが、鍵を伝送することができる。可能な鍵のサーバには、起点のサーバ、特殊化された鍵サーバ、信頼されるエッジサーバ、または以上のサーバの任意の組み合わせが含まれる。

【0017】さらに、本発明は、データをクライアントに転送することができる速度の推定を企図している。起点のサーバと信頼されるエッジサーバの間、または信頼されるエッジサーバとクライアントの間、またはパス全体の接続の待ち時間を監視する、または計算することができる。接続待ち時間の経験上の推定値、または理論上の推定値に基づき、各クライアントに関して配信のため

の時間のデータベースを集約することができる。サーバが、この配信時間を使用して、暗号化されたデータ、暗号解読されたデータ、または鍵の伝送をどれだけすぐに開始する必要があるかを判定することができる。例えば、信頼されるエッジサーバが、ローカルでデータを記憶する、または暗号解読する能力を有していない自らのクライアントのすべてに対し、そのクライアントのすべての最小伝送時間をイベントがリリースされるべき時刻から引くことによって計算された時刻に、暗号解読されたデータの伝送を開始することが可能である。替わりに、信頼されるエッジサーバは、各クライアントへのイベントの伝送を、その特定のクライアントへの伝送時間だけをイベントがリリースされるべき時刻から引き、これにより、個々の接続の待ち行列を考慮に入れることによって計算された時刻に開始することができる。サーバが、この後者の演算を行うことができる場合、関心を有するクライアントはそれぞれ、イベントがリリースされるべき時刻に非常に近接してイベントを受け取り、一方、前者の演算は、より変化のある着信時刻をもたらす。公正さおよび効率をさらに高めるため、まず、クライアントをサーバ間で再配分して、待ち時間の一部の源の影響を減じること、および一部の状況で、同様の接続速度を有するクライアントを同じサーバに配置する（これにより、時差的な配信をより効果的にする）ことが可能である。これにより、特定のクライアントーサーバ伝送時間の推定値に応じて、いくつかの異なって配置され接続されたクライアントによるイベントのほぼ同時の獲得を可能にすることができる。

【００１８】本発明のさらなる特徴および利点は、添付の図を参照して進められる例示の実施形態の以下の詳細な説明から明白となる。

【００１９】

【発明の実施の形態】頭記の特許請求の範囲は、詳細とともに本発明を提示しているが、本発明、ならびに本発明の目的および利点は、添付の図面と合わせて考慮した以下の詳細な説明から理解することができる。

【００２０】本発明は、クライアントが、できる限り同時刻にイベントを受け取り、またその時点を過ぎるとイベントがもはや有意義でなくなる、またはイベントに含まれる情報が陳腐になる時間フレームの終了の前に、できる限り多くのクライアントがイベントを受け取るような方法でクライアントの集合にイベントを配信するための方法、コンピュータ可読媒体、およびシステムを目的とする。具体的には、本発明は、イベントがリリースされる時刻より前に暗号化されたイベントを送信することを企図している。暗号化されたイベントは、クライアントまたはサーバにおいて記憶することができる。イベントがリリースされるべき時刻に、暗号解読の鍵を各クライアントまたはサーバに送信することができる。鍵は、小さい可能性が高いので、鍵の伝送時間は、比較的短く、各クライアントが、鍵を受け取り、これにより、ほぼ同時刻にデータを暗号解読する能力を受け取る。クライアントが、暗号化されたイベントを記憶する能力、または暗号化されたイベントを暗号解読する能力を有していない場合、暗号化されたイベントは、サーバにおいて記憶し、暗号解読して、次に、クライアントに送信することができる。信頼されるエッジサーバが、クライアントのためにイベントを暗号解読する場合、リリース時刻より前に鍵を送信することができる。また、クライアントと信頼されるエッジサーバの間の接続における計算された待ち時間、または測定された待ち時間を考慮に入れるようにリリース時刻より前にクライアントへの暗号解読されたイベントの送信を開始することができる。替わりに、クライアントのためにイベントを暗号解読するサーバが、信頼されるエッジサーバではない場合、サーバは、リリース時刻に、またはリリース時刻の後に鍵を受け取り、イベントの暗号解読を完了すると、クライアントに暗号解読されたイベントを送信することができる。

暗号化されたイベントを十分に早期に送信することができない場合、すなわち、リリース時刻より前に暗号化されたイベントの受信を完了するだけ十分に早期に暗号化されたイベントを送信することができない場合、鍵の伝送を遅延させて、クライアントが、暗号化されたイベントの受信を終えることができるようにする。鍵は、遅延および揺らぎを考慮に入れた場合、終了時刻から鍵の伝送時間を引いたものに等しいとをさらに含む。時刻に送信することができる。マルチキャスティンググループ通信プロトコルを使用して独立したセッションの数を最小限に抑えることができる。鍵のサイズが比較的小さいため、相当な冗長性を使用して、マルチキャスティングを介してでも鍵の適切な配信を確実にすることができる。

【００２１】図を参照して、同様の符号が同様の要素を示すが、本発明をサーバ計算環境のコンテキストで以下に説明する。本発明を実施するのに必須ではないが、本発明は、サーバまたはクライアントの計算デバイスによって実行されるプログラムモジュールなどのコンピュータ実行可能命令によって実施されるものとして説明する。一般に、プログラムモジュールには、特定のタスクを実行するか、抽象データタイプを実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造等が含まれる。

【００２２】本発明は、サーバ以外のコンピュータシステム構成で実施してもよい。例えば、本発明は、ルータ、マルチプロセッサシステム、パーソナルコンピュータ、家庭用電化製品、ミニコンピュータ、メインフレームコンピュータ等において実現することもできる。また、本発明は、タスクが、通信網を介してリンクされた遠隔処理デバイスによって行われる分散計算環境で実施してもよい。分散計算環境では、プログラムモジュールが、ローカルのメモリ記憶デバイスと遠隔のメモリ記憶デバイスの両方に配置されていることが可能である。

【００２３】本発明は、上述のように、多数のタイプの計算環境に組み込むことができるが、本発明の以下の詳細な説明は、従来のサーバ２０の形態の例としての汎用計算デバイスのコンテキストで提示する。

【００２４】本発明を詳細に説明する前に、本発明が機能する計算環境を図１に関連して説明する。サーバ２０は、処理ユニット２１と、システムメモリ２２と、システムメモリから処理ユニットまでを含む様々なシステム構成要素を結合するシステムバス２３とを含む。システムバス２３は、様々なバスアーキテクチャの任意のものを使用するメモリバスまたはメモリコントローラ、周辺バス、およびローカルバスを含むいくつかのタイプのバス構造の任意のものとすることが可能である。システムメモリには、読取り専用メモリ（ＲＯＭ）２４およびランダムアクセスメモリ（ＲＡＭ）２５が含まれる。始動中などに、サーバ２０内部の要素間で情報を転送するのを助ける基本ルーチンを含む基本入力／出力システム（ＢＩＯＳ）２６が、ＲＯＭ２４の中に記憶される。サーバ２０は、ハードディスク６０に対して読取りおよび書込みを行うためのハードディスクドライブ２７と、取外し可能な磁気ディスク２９に対して読取りおよび書込みを行うための磁気ディスクドライブ２８と、ＣＤ ＲＯＭまたはその他の光媒体などの取外し可能な光ディスク３１に対して読取りおよび書込みを行うための光ディスクドライブ３０とをさらに含む。

【００２５】ハードディスクドライブ２７、磁気ディスクドライブ２８、および光ディスクドライブ３０はそれぞれ、ハードディスクドライブインターフェース３２、磁気ディスクドライブインターフェース３３、および光ディスクドライブインターフェース３４でシステムバス２３に接続される。以上のドライブおよび関連するコンピュータ可読媒体により、コンピュータ可読命令、データ構造、プログラムモジュール、および他のデータの不揮発性ストーレッジが、サーバ２０に提供される。本明細書で説明する例としての環境は、ハードディスク６０、取外し可能な磁気ディスク２９、および取外し可能な光ディスク３１を使用するが、磁気カセット、フラッシュメモリカード、デジタルビデオディスク、ベルヌーイカートリッジ、ランダムアクセスメモリ、読取り専用メモリなどの、コンピュータによってアクセス可能な、データを記憶することができる他のタイプのコンピュータ可読媒体も例としての動作環境において使用できることが、当分野の技術者には理解されよう。

【００２６】オペレーティングシステム３５、１つまたは複数のサーバプログラム３６、他のプログラムモジュール３７、およびプログラムデータ３８を含め、いくつかのプログラムモジュールをハードディスク６０、磁気ディスク２９、光ディスク３１、ＲＯＭ２４またはＲＡＭ２５の上に記憶することができる。ユーザは、キーボード４０やポインティングデバイス４２などの入力デバイスを介してサーバ２０にコマンドおよび情報を入力することができる。その他の入力デバイス（図示せず）には、マイクロホン、ジョイスティック、ゲームパッド、サテライトディッシュ、スキャナ等が含まれることが可能である。以上の入力デバイスおよび他の入力デバイスは、しばしば、システムバスに結合されたシリアルポートインターフェース４６を介して処理ユニット２１に結合されるが、パラレルポート、ゲームポート、またはユニバーサルシリアルバス（ＵＳＢ）ポートなどの他のインターフェースで接続してもよい。また、モニタ４７、または他のタイプの表示デバイスも、ビデオアダプタ４８などのインターフェースを介してシステムバス２３に接続することができる。

上のコンテキストで説明するが、以下

【００２７】サーバ２０は、ルータ４９のようなハードウェアまたは他のネットワーク機器を介する１つまたは複数の遠隔クライアント５０または追加のサーバ５２への論理接続を使用するネットワーク化された環境で動作する。遠隔クライアント５０は、パーソナルコンピュータ（ＰＣ）、ネットワークＰＣ、ピアデバイス、他の一般的なネットワークノード、または他の計算デバイスであることが可能であり、通常、サーバ２０に関連して前述した要素の多くを含む。遠隔サーバ５２は、メールサーバ、大きい可能性が高くミラーサーバ、Ｗｅｂサーバ、または他の一般的なネットワークノードであることが可能であり、通常、サーバ２０に関連して前述した要素の多く、またはすべてを含む。ネットワークルータ４９は、ワンだけに（one-armed）ルータ、エッジルータ、マルチホームルータ、ソフトウェアアプリケーションルータ、または他の一般的なネットワークノードであることが可能であり、通常、パケットが転送されるべきネットワークにおける次のポイントを決定する。図１に描いた論理接続５１は、ローカルエリアネットワーク（ＬＡＮ）および／またはワイドエリアネットワーク（ＷＡＮ）であることが可能である。そのようなネットワーキング環境は、オフィス、企業全体のコンピュータ網、イントラネットおよびインターネットにおいて一般的である。

【００２８】ＬＡＮまたはＷＡＮのネットワーキング環境で使用されるとき、サーバ２０は、ネットワークインターフェースまたはネットワークアダプタ５３を介してネットワーク５１に接続される。ネットワーク化された環境では、サーバ２０に関連して描いたプログラムモジュール、またはプログラムモジュールの部分が、ネットワークルータ４９を介してアクセスされる遠隔のメモリ記憶デバイスの中に記憶されることが可能である。図示したネットワーク接続は、例としてのものであり、コンピュータ間で通信リンクを確立する他の手段も使用できることを理解されたい。

【００２９】以下の説明では、本発明は、特に明示しない限り、１つまたは複数のコンピュータによって行われる動作および記号表現のオペレーションに関連して説明

する。このため、ときとして、コンピュータによって実行されるものとして述べられるそのような動作およびオペレーションには、コンピュータの処理ユニットによる、構造化された形態のデータを表す電気信号の操作が含まれることが理解されよう。この操作は、データを変形するか、またはコンピュータのメモリシステムの中の場所にデータを保持し、データは、当分野の技術者にはよく理解されている方法でコンピュータのオペレーションを再構成するか、または別の方法で変更する。データが保持されるデータ構造は、メモリ、すなわち、データフォーマットによって定義される特定のプロパティを有するメモリの物理的な場所である。ただし、本発明を以上のコンテキストで説明するが、以下に説明する種々の動作およびオペレーションをハードウェアで実施してもよいが当分野の技術者には認識されるとおり、これに、限定することを意図するものではない。

【００３０】本発明の一態様によれば、ネットワークに接続された１組のクライアントに、イベントのリリース時刻より前に暗号化されたイベントが提供され、その後、リリース時刻に、またはリリース時刻の後に、そのイベントを暗号解読するために暗号解読の鍵が提供される。イベントは、大きい可能性が高く、ナローバンド接続を介して接続されたクライアントに送信するのに相当な時間を要し、一方、ブロードバンド接続を有するクライアントは、比較的速やかにそのイベントを受信することができる。ブロードバンドのクライアントは、ナローバンドのクライアントより前にイベントに含まれる情報へのアクセスを得ることになり、ナローバンドのクライアントにとって不利になるようにその情報を使用することができるので、暗号化されていないイベントの配信は、不公正である。しかし、イベントを暗号化し、リリース時刻より前にイベントを送信することにより、配信の公正さを実現することができる。というのは、暗号解読の鍵が比較的小さく、鍵の伝送は非常に短い時間量であることが可能であるため、大幅に異なる接続速度の間でも、クライアントのそれぞれが、狭い時間幅の中で暗号解読の鍵を受け取ることができるからである。したがって、各クライアントが、狭い時間幅の中でイベントに含まれる情報へのアクセスを得て、公正な配信が提供される。

【００３１】明らかなように、配信の公正さを確実にするためには、暗号解読の鍵より前に暗号化されたイベントが受信されなければならない。そうでなければ、クライアントは、鍵を有するが、暗号解読するげきイベントを有さないからである。ただし、これは、すべてのケースで保証することができない。したがって、本発明は、クライアントに信頼できるように配信するのに十分なだけ前もって起点のサーバから暗号化されたイベントを入手できる場合、所望される場合は、リリース時刻に、またはリリース時刻の後に暗号解読の鍵を送信することを企図している。また、本発明は、リリース時刻の後、終了時刻から鍵を配信するのに必要な遅延時間を引いたものに等しい時刻までの任意の時刻に暗号解読の鍵を送信することも企図している。したがって、鍵を送信することを遅延させて、鍵を送信する前にできる限り多くのクライアントが暗号化されたイベントの受信を終えることができるようにすることが可能である。したがって、起点のサーバが、クライアントがリリース時刻より前に暗号化されたイベントを受信することができるようにするのに十分なだけ早い時刻に、暗号化されたイベントを送信することができない場合、またはそうすることが許されない場合、必要に応じて鍵を送信するのを遅延させて、イベントに含まれる情報への可能な限り公正なアクセスを提供することができる。

【００３２】本発明の別の態様によれば、暗号化されたイベントをサーバに送信し、クライアントに送信する前にサーバにおいて暗号解読することができる。そのようにすると、個々のクライアントが、極めて大きい可能性がある暗号化されたイベントを保持する必要がなく、またイベントを暗号解読することによって自らの処理システムに負担をかける必要もない。信頼されるサーバは、ネットワーク中のサーバ、すなわち、リリース時刻より前にイベントをリリースしない起点のサーバにより信頼される、ネットワーク中のサーバである。信頼されるエッジサーバは、起点のサーバと信頼することができる種々なレベルの機能をクライアントの間の論理接続における最後のサーバである。ネットワークでは、サーバ、したがって、信頼されるネットワークのエッジを考えることができる。クライアントのためにイベントを暗号解読するサーバが、信頼されるエッジサーバである場合、その信頼されるエッジサーバが、リリース時刻より前に暗号化されたイベントおよび鍵の提供を受けるので、リリース時刻より前にイベントを暗号解読することが可能である。替わりに、クライアントのためにイベントを暗号解読するサーバが、信頼されるエッジサーバではない場合、鍵は、リリース時刻の後に、またはリリース時刻より十分に前に送信して、そのサーバが、イベントを暗号解読してクライアントに伝送できるようにすることが可能である。しかしながら、このサーバは暗号解読したイベントを保持して指定された時刻まで待機することを信頼することはできない。いずれの場合も、暗号解読されたイベントは大容量であろうが、ナローバンドのクライアントに伝送するのに相当な時間量を要するという問題が残る。ブロードバンドのクライアントがイベントを受信するときと、ナローバンドのクライアントがイベントを受信するときの間の時間の差を最小限に抑えるため、信頼されるエッジサーバは、ナローバンドのクライアントにリリース時刻より前にイベントを送信し、双方のクライアントが、ほぼ同時刻にイベントを受信することができるようにすることができる。

【００３３】本発明のさらに別の態様によれば、暗号化

されたイベントおよび暗号解読の鍵をマルチキャスティングプロトコルを使用して送信して、ネットワーク効率を高め、伝送の負担を分散させることができる。当分野の技術者には周知のとおり、マルチキャスティングは、しばしば、伝送されたデータが失われた場合、または壊れた場合、再送を要求する効率的なメカニズムを提供しない。鍵は、極めて小さい可能性があるため、相当な冗長性とともに鍵を送信し、これにより、再送が必要となる確率を最小限に抑える方が効率的である可能性がある。例えば、ナローバンドのクライアントにとってさえ、極めて小さく、効率的に伝送することが可能な単一のメッセージで鍵の複数のコピーを送信することができる。替わりに、起点のサーバ、信頼されるエッジサーバ、特殊化された鍵サーバ、または以上のサーバの任意の組み合わせを含め、異なる鍵サーバからなど、異なるネットワークルータを介して鍵の単一のコピーを送信することができる。

【００３４】本発明によれば、図２は、例としてのネットワーク化された環境を示している。重要なことには、本発明は、何らかの特定のネットワークプロトコルでの実施に限定されないことである。本発明は、例えば、ＴＣＰ／ＩＰプロトコル、ＡｐｐｌｅＴａｌｋプロトコル、Ｎｏｖｅｌｌプロトコルを使用して、またコンテンツ配信網で実施することができる。以上のプロトコルは、もちろん、様々なレベルの機能を提供する。したがって、一部のネットワークでは、サーバのソフトが、より多くの機能を行うことが可能であり、一方、他のネットワークでは、サーバのソフトウェアが、基礎のプロトコルに依拠してその機能を提供することが可能である。本発明の例としての実施形態を説明する際、必要とされる特定の情報または機能が、基礎のプロトコルにより、またはサーバ上またはクライアント上のソフトウェアにより提供されることが可能である。基礎の方法は、不変のままであり、単に既存の機能を組み込んで必要とされるタスクを完了することができる。

【００３５】図２は、本発明の例としての実施形態を説明することができるネットワーク環境２００を示している。起点のサーバ２１０が、信頼されるエッジサーバ２２０、２２１、および２２２、ならびにサーバ２３０、２３１、および２３２などの信頼されない追加のサーバを含むネットワークに接続されている。また、このネットワークは、クライアントマシンに論理接続されているパーソナル計算デバイス（ＰＣ）の形態でクライアントも含む。クライアント５０は、例えば、ナローバンド接続２３８を介して接続されていることが可能であり、またクライアント１５０は、ブロードバンド接続２３９を介して接続されていることが可能である。当分野の技術者には周知のとおり、ナローバンド接続は、一般に、５６ｋｂｐｓまたは３３．６ｋｂｐｓなどの一般的に使用されるアナログモデム速度のダイヤル呼出し接続である。ブロードバンド接続は、ケーブルモデム、デジタル加入者回線（ＤＳＬ）モデム、またはサテライトモデムなどの任意の数の技術を介して行うことができ、一般に、ナローバンド接続より格段に高いスループットを提供する。

【００３６】好適実施形態では、イベントが、起点のサーバ２１０を起点とする。イベントは、クライアント５０および１５０に配布されるデータの任意の集合であることが可能である。例えば、イベントは、単純な場合、政府の会計局または会計部門からの経済ニュースのリリースであることが可能であり、あるいは企業からの新しい製品またはサービスのリリースを供覧するデジタル動画、または人気のある音楽家または音楽グループからのそのようなクライアント新しい音楽ビデオのリリースのように、相当により大きくネットワーク帯域幅を、より複雑であることが可能である。一般に、イベントは、[illegible]トは、リリース時刻に先立つ配布が、不適切であるような性質のものである。例えば、政府の経済データが、リリース時刻より前に配布されたとしたら、金融市場が混乱させられる可能性がある。同様に、新しい音楽ビデオが、リリース時刻より前にリリースされたとしたら、そのビデオのマーケティングが需要を生み出すのに十分な時間がとれていない可能性があり、ビデオが失敗であるとみなされる可能性がある。また、イベントは、一般に、配信の公正さが重要であるような性質のものである。[illegible]の例示として提示する。したがって、政府の経済データが、他のクライアントより前に一部のクライアントにリリースされたとしたら、[illegible]ら、そのデータを受け取っていたクライアントは、そのブロードバンドのクデータを使用して、そのデータをまだ受け取っていなかったクライアントから利益を上げる可能性がある。同様に、１つのグループのクライアントが、別のグループより前に新しい音楽ビデオを受け取ったとしたら、配信の不公正さに焦点を当てる何らかのメディアの注目によ[illegible]り、ビデオ自体の品質に関するより好意的な世間の関心[illegible]がそらされる可能性がある。したがって、本発明は、異なる帯域幅および異なる計算能力のクライアント間など[illegible]における、公正な方法での情報またはイベントの配信を[illegible]企図している。

【００３７】また、クライアントに配信されるイベント[illegible]に含まれる情報も、しばしば、その時点を過ぎると情報が陳腐になる、または有意義でなくなる終了時刻を有する。政府経済報告などの一部のデータの場合、情報は、次の報告が出されるまで、１ヶ月間、またはそれより長い期間、最新である可能性がある。同様に、新しい音楽ビデオは、数週間、最新であると見なされる可能性がある。あるいは、クライアントに配信されることが可能な一部のデータは、非常に急速にその意義を失う可能性がある。例えば、所与のエリアに関する気象レーダの時間経過を示す動画は、１５分だけ最新であることが可能である。本発明は、公正な方法で、またその時点を過ぎるとイベントに含まれる情報が、クライアントにとって有

用でなくなる可能性がある終了時刻より前にイベントを配信することを企図している。

【００３８】図３を参照すると、本発明によって企図されるイベントの時系列が示されている。棒グラフ３００は、特定のサーバのクライアントのグループを表している。したがって、例えば、このグラフは、ナローバンドのクライアント５０とブロードバンドのクライアント１５０の両方が接続されている信頼されるエッジサーバ２２１、またはやはりナローバンドのクライアント５０とブロードバンドのクライアント１５０が接続されている外部の（信頼されない）サーバ２３２を表していることが可能である。図２は、サーバ２２１および２３２に接続されたいくつかのそのようなクライアントだけを示しているが、同様のネットワーク接続を介してさらに多くのクライアントを接続できることを理解されたい。棒グラフ３００で、通常は連続関数である配信の時間が、図示するカテゴリに入るように近似されている。したがって、左端に図示する第１のグループのクライアント３１０は、およそ５秒ないし１５秒の時間範囲内にメッセージを受信し、第２のグループ３１２は、４０秒から６０秒の時間範囲内にメッセージを受信し、以下同様である。棒グラフ３００で示した時間は、直線的に増分されていないことに留意するのが重要である。これは、伝送時間が、単に本発明の例示として提示されているためである。

【００３９】棒グラフ３００から明らかなように、図示したサーバには、ブロードバンドのクライアントおよびナローバンドのクライアントを含め、およそ１００のクライアントが接続されている。棒グラフ３００は、サーバが暗号化されたイベントの送信を開始する時刻３５０で開始する。サーバは、いくつもの理由で時刻３５０に暗号化されたイベントの送信を開始することが可能である。例えば、時刻３５０は、サーバが、図２に示した起点のサーバ２１０のような起点のサーバから暗号化されたイベントを受け取った最初の時刻であることが可能である。替わりに、時刻３５０は、サーバが、起点のサーバから暗号化されていない形態でイベントを受信した場合、イベントを暗号化するのを完了した最初の時刻であることが可能である。また、サーバは、起点のサーバからの明示的な命令の故に、時刻３５０で暗号化されたイベントの送信を開始していることも可能である。暗号化されたイベントの伝送は、特定の時刻を待つ必要がないため、信頼されるエッジサーバと信頼されないサーバの両方を使用してイベントを配信できることに留意されたい。

【００４０】イベントを受信する最初のセットのクライアント３１０は、時刻３５０のおよそ１０秒後に受信し、一方、最後のセットのクライアント３２６は、およそ７００秒後にイベントを受信する。そのような大きい相違から明らかなように、リリース時刻にクライアント

に単に暗号化されていないイベントを送信することにより、クライアント３１０のような最初のクライアントが既にイベントを受信してから１１分間より長い時間が経ってからでないと、クライアント３２６のような一部のクライアントはイベントを受信しない。イベントが、政府の経済データのリリースであったとすると、クライアント３１０は、まだ情報を受信していないクライアント３２６から利益を上げるのに十分な時間を有していたことになる。当分野の技術者には理解されるとおり、棒グラフ３００は、比較的小さいイベントの配信を示している。というのは、ブロードバンドのクライアントがこのイベントを１０秒間ほどの短い時間でダウンロードすることが可能だからである。新しい製品を供覧するビデオなどのより大きいイベントの場合、最も高速のクライアント３１０でさえ、数分間、そのイベントを受信しなければ、利用可能にならない可能性があり、最も低速のクライアント３２６は、そのようなイベントを受信するのに数時間かかる可能性がある。

【００４１】図３に示すとおり、サーバは、すべてのクライアントが、暗号化されたイベントを受信しているのに十分なだけリリース時刻３６０より前の時刻３５０に、そのデータ暗号化されたイベントの送信を開始する。次に、図３において示すとおり、時刻３６０に等しいか、または後の時刻であることが可能な時刻３７０に、以下にさらに説明するとおり、サーバが、時刻３５０に送信された暗号化されたイベントを暗号解読する鍵を送信することができる。当分野の技術者には認められるとおり、厳密に新与の時間に機能を行うのは非常に困難である。というのは、すべての計算デバイスが、別々のサイクルで動作するからである。それでも、本発明では、リリース時刻３６０直後の時刻をリリース時刻３６０にほぼ等しいものと見なしている。鍵のサイズが小さいため、ナローバンドのクライアントにとってさえ、鍵を受信するのにかかる時間の相違は、ほとんど存在しない。したがって、図３に示すとおり、クライアント３３０のすべてが、ほぼ同時刻に鍵を受信する可能性が高い。クライアントのセット３３０は、セット３１０ないし３２６で暗号化されたイベントを受信したのと同じ１００のクライアントを示し、時刻３７０より前の時刻時刻３７０にこのクライアントに追加のデータ、すなわち、鍵を送信する。すなわち、暗号解読の鍵が送信され、棒３３０で示されるとおり、クライアントのすべてがその鍵を２秒間以内に受信することだけが異なっている。したがって、各クライアントは、リリース時刻３６０のすぐ後にほぼ同時刻に暗号解読の鍵を使用してイベントを暗号解読することにより、イベントに含まれる情報へのアクセスを初めて受け取る。

【００４２】イベントは暗号化されているので、信頼されるエッジサーバ２２１のような信頼されるエッジサーバと、信頼されないサーバ２３２のような信頼されないサーバの両方を使用して、リリース時刻３６０より前にイベントを配信することができる。ただし、以下により

詳細に示すとおり、暗号解読された、または暗号化されていないイベントが伝送される場合、リリース時刻３６０より前に信頼されるエッジサーバが、そのイベントを保持することができる。ただし、信頼されないサーバが、リリース時刻より前にイベントをリリースする可能性がある。暗号化されたイベントの場合、信頼されないサーバがリリース時刻より前にイベントをリリースすることに起因してもたらされる不公正さは存在しない。というのは、クライアントが、イベントに含まれる情報にアクセスするのに必要な鍵を有さないからである。しかし、暗号解読された、または暗号化されていないイベントの場合、個々のサーバによるリリース時刻に先立つリリースにより、イベントに含まれる情報への不平等なアクセスがもたらされる可能性がある。したがって、明らかなように、データは、利用可能になるとすぐにクライアント５０や１５０のようなクライアントに送信することができる。そのようなデータが、暗号解読の鍵、暗号化されていないイベント、またはクライアントがイベントに含まれる情報に対するアクセスを受取可能にするその他のデータを含むとき、そのデータを最も近接した信頼されるサーバにおいて保持し、適切なときにリリースすることができる。信頼されないサーバは、データをリリースするのに適切な時刻までデータを保持するものと信頼できない可能性がある。上記に説明したとおり、最も近接した信頼されるサーバが、信頼されるエッジサーバである。

【００４３】暗号解読の鍵を、鍵サーバによって送信することが可能である。鍵サーバは、鍵を送信する任意のサーバとすることが可能であり、鍵サーバには、起点のサーバ、１つまたは複数の信頼されるエッジサーバ、特殊化された中央鍵サーバ、または分散されたグループの特殊化された鍵サーバ、または以上のサーバの任意の組み合わせを含むことが可能である。また、中央鍵サーバ、または分散型の特殊化された鍵サーバは、ネットワーク環境２００の一部とすることも可能であり、時刻３７０にクライアントに直接に鍵を伝送することができるか、または時刻３７０より前の時刻に信頼されるエッジサーバ２２１に対して鍵を配信することができ、鍵の送信時刻に関する命令を提供することができる。ただし、信頼されないサーバ２３２に対しては、時刻３７０より前にではなく、時刻３７０に鍵を送信することができる。というのは、サーバ２３２は、時刻３７０まで鍵を保持すると信頼することができないからである。できる限り多くのクライアントにできる限り効率的に鍵が着信することを確実にするのに、鍵をクライアントに配信する多数の異なるネットワークパスを使用して、前述したサーバのような複数のサーバから鍵を伝送することが有益である。複数のパスを使用することにより、何らかの単一のパスに輻輳が生じ、鍵の受信を遅延させる可能性のリスクが小さくなる。以下に説明するとおり、鍵の伝送は、クライアントによる暗号化されたイベントの受信に依存する可能性があるので、サーバ群と中央鍵サーバの間の通信、またはサーバ群と鍵サーバのネットワークの間の通信が、クライアントへの鍵の送信を調整するように企図される。

【００４４】イベントに関して使用される暗号化は、データ暗号化標準（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）（ＤＥＳ）、セキュアアンドファースト暗号化ルーチン（Ｓｅｃｕｒｅ Ａｎｄ Ｆａｓｔ Ｅｎｃｒｙｐｔｉｏｎ Ｒｏｕｔｉｎｅ）（ＳＡＦＥＲ）、国際データ暗号化アルゴリズム（Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ａｌｇｏｒｉｔｈｍ）（ＩＤＥＡ）、ならびにＴｗｏｆｉｓｈ、ＳＥＲＰＥＮＴ、ＲＣ６、およびＭＡＲＳなどのアドバンスト暗号化標準（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）（ＡＥＳ）候補のいずれかを含め、普及している暗号化方法のいずれか１つ、または組み合わせとすることが可能である。本発明は、様々なブロードバンドのクライアントおよびナローバンドのクライアントへの伝送時間に大きな違いが存在しないように、サイズが比較的小さい１つまたは複数の暗号化されたイベントが、解読の鍵で暗号解読することができる任意の暗号化方法の使用を企図している。

【００４５】図４を参照すると、イベント配信が一様な速度を維持しておらず、ラフ４００として示されている。図３と同様に、サーバＡが、終了時刻５９０までは、信頼されるエッジサーバ２２１のような信頼されるエッジサーバであるか、または配信されるイベントが暗号化されているため、信頼されないサーバ２３２のような信頼されない特定などの信頼されないサーバであることが可能である。明らかなように、サーバが、イベントの送信を開始した時刻４００は、時刻４５０は、各クライアントが、暗号化されたイベントを受信できるようにするだけ十分にリリース時刻４６０より前ではなかった。時刻４５０は、サーバによって起点のサーバからイベントが受信された時刻に依存している可能性がある。サーバが、時刻４５０に暗号化されたイベントの送信を開始したときからリリース時刻４６０までの時間が短いため、クライアント４２４および４２６は、リリース時刻に暗号化されたイベントの受信をまだ完了していない。そのような状況では、本発明は、クラスタのすべてのクライアントのすべてが、暗号化されたデータを受信するまで鍵の伝送を遅延させることを企図している。ただし、鍵の伝送は、鍵が終了時刻４９０より後に受信されるほど遅延させてはならない。さらに、実用性の配慮も考慮に入れられる。したがって、わずかなパーセンテージのユーザが、暗号化されたデータをまだ受信するのを終えていないが、鍵を伝送して、大多数のユーザが、リリース時刻に近い時刻にデータを受け取ることができるようにするのが可能である。そのような配慮は、以下により詳細に示すとおり、ネットワーク全体でイベントの公正な配信を可能にするように複数のサーバを有するネット

ワークでは特に重要である。

【００４６】図４で示すとおり、本発明は、リリース時刻４６０の後であり、最後のグループのクライアント４２６が、暗号化されたイベントの受信を終えた後の時刻４７０に暗号解読の鍵を送信することを企図している。また、鍵が送信される時刻４７０は、すべてのクライアント４３０が、終了時刻より前に鍵を受け取ることができるように、終了時刻４９０より十分に前でもある。図４では、鍵が送信される時刻４７０は、最後のグループのクライアント４２６が、暗号化されたイベントを受信した後すぐに来るように示しているが、すべてのクライアント、またはできる限り多くのクライアントが、鍵を受け取り、これにより、終了時刻４９０より前にイベントに含まれる情報へのアクセスが与えられるよう、終了時刻４９０より十分に前の任意の時刻に、鍵を送信することができる。

【００４７】図５を参照すると、棒グラフ５００として示すイベント配信が、本発明によって企図される別の伝送シーケンスを示している。図５で示すとおり、終了時刻５９０より後でもセットのクライアント５２４および５２６によって暗号化されたイベントがまだ受信されている。この場合も信頼されるエッジサーバおよび信頼されないサーバを含むサーバは、時刻５５０まで暗号化されたイベントの送信を開始しておらず、時刻５５０は、クライアントのすべてが、終了時刻５９０より前に暗号化されたイベントを受信できるようにするには遅すぎる。この場合も、時刻５５０は、サーバが起点のサーバからイベントを受信した時刻などの外部要因によって規定されている可能性がある。図５では、送信時刻５５０をリリース時刻５６０と等価であるものとして示しているが、送信時刻５５０は、リリース時刻５６０より前であるか、またはリリース時刻５６０の後であることも可能であり、それでも、終了時刻５９０が過ぎるまで暗号化されたイベントの受信を完了していないセットのクライアントが生じる可能性がある。

【００４８】そのような状況では、本発明は、信頼されるエッジサーバが、できる限り多くのクライアントが、暗号化されたイベントの受信を終えていることを確実にするように暗号解読の鍵の送信をできる限り長い間、待つことができるのを企図している。したがって、鍵がクライアントによって受信可能にするだけ十分に終了時刻５９０より前の時刻５７０に、信頼されるエッジサーバが、鍵の送信を開始することができる。図５で示すとおり、信頼されるエッジサーバは、セット５２４および５２６の中のクライアントが、暗号化されたデータの受信を完了する前に、時刻５７０に鍵の送信を開始することができる。終了時刻５９０までには、クライアントのそれぞれが、暗号解読の鍵を受信しているが、クライアント５２４および５２６は、イベントの中で送信されたデータにその鍵を使用してアクセスできるにはまず、暗号

化されたイベントの受信を完了する必要がある。しかし、セットのクライアント５１０ないし５２２は、時刻５７０における鍵の伝送より前に暗号化されたイベントを既に受信しており、終了時刻５９０の前にイベントに含まれるデータにアクセスすることができる。さらに、クライアント５１０ないし５２２はそれぞれ、データへのこのアクセスをほぼ同時刻に受け取り、信頼されるエッジサーバに接続されたクライアントの待ち時間を所与として、可能な限り公正な情報の配信が提供されている。

【００４９】図２に示したサーバのクライアント５０および１５０の一部が、暗号化されたイベントを記憶するのに十分な記憶スペースを有していなくてもよいことを企図している。ただしたは暗号化されたイベントを暗号解読するのに十分な処理能力を有していなくてもよい。さらにクライアントやサーバは、信頼されるが、イベントを記憶し、暗号解読する能力は、イベントにより異なる可能性がある。例えば、政府の経済データのリリースなどの比較的小さいイベントは、容易に記憶し、暗号解読することができ、多くのクライアントが、十分な記憶スペースおよび十分な処理能力を有する可能性が高い。しかし、デジタル動画の場合、または他の大きいイベントの場合、より小さいイベントに対応することができたクライアントを含め、多くのクライアントが、十分な記憶スペースまたは十分な処理能力を有さない可能性がある。

【００５０】したがって、本発明は、サーバが、暗号化されたイベントを送信し、続いて暗号解読の鍵を送信できるか、または信頼されるエッジサーバがイベントをローカルで暗号解読し、イベントの暗号解読されたバージョンを伝送できることを企図している。言い換えると、起点のサーバが、暗号化されていないイベントを送信する場合、信頼されるエッジサーバは、イベントを暗号化することができず、記憶能力または処理能力を欠いているかもしれない１００のクライアントに暗号化されていないイベントを送信することができる。当分野の技術者には分かるとおり、暗号化されていないイベントを表すデータは、暗号解読されたイベントと同じ情報を含む。イベントの完全性を確実にするため、暗号解読されたイベントを受信するクライアントは、リリース時刻５６０より前にそのイベントを受信してはならないことを前に説明したとおりである。したがって、信頼されるエッジサーバが、リリース時刻まで暗号化されたイベントを受信し、次に暗号解読されたイベントを保持することができるが、または信頼されるエッジサーバが、サーバが暗号解読されたイベントを送信することを必要とするクライアントへの待ち時間を判定し、そのクライアントが、リリース時刻に暗号解読されたイベントを受信するように、リリース時刻より前に暗号解読されたイベントの送信を開始する。

【００５１】図２に戻ると、信頼されるエッジサーバ２２１に、ブロードバンド接続を介して接続されるパーソナル計算デバイス１５０が接続され、またナローバンド接続を介して接続されるさらに２つのパーソナル計算デ

バイス５０が接続されていることが示されている。２つのパーソナル計算デバイス５０が、暗号化されたイベントを記憶し、暗号解読するのに十分な記憶スペースおよび十分な処理能力を欠いている場合、暗号化されたイベントは、信頼されるエッジサーバ２２１によって暗号解読されることが可能であり、その暗号解読されたイベントを計算デバイス５０に送信することができる。

【００５２】図3は、信頼されるエッジサーバ２２１のようなサーバの１００のクライアントへの暗号化されたイベントの伝送を示した。図3は、クライアントに送信されるイベントが暗号化されているので、信頼されないサーバの使用を企図したが、図6は、信頼されるエッジサーバの使用を企図している。ただし、図2に示すとおり、信頼されるエッジサーバ２２０および２２２のような信頼されるエッジサーバは、信頼されないサーバ２３０および２３１のようなさらなる信頼されないサーバを介してクライアントと通信することが可能である。信頼されるエッジサーバ２２０および２２２は、以下に示すとおり、適切な時刻に暗号化されていないイベントを送信することによって配信の公正さを維持しながら、起点のサーバ２１０と最終のクライアント宛先の間で暗号化されていないイベントを伝送することができる限界である。また、図6は、例示することだけを意図し、信頼されるエッジサーバ２２１に接続される１５０のクライアントへの本発明によって企図される伝送を示している。具体的には、図6は、図3に示したのと同じ１００のクライアントに暗号化されたイベントおよび暗号解読の鍵を送信することを示し、またさらに、十分な記憶能力または十分な処理能力を有さない５０の新たなクライアントに暗号解読されたイベントを送信することを示している。

【００５３】図6は、暗号化されたイベントを記憶し、暗号解読することができる１００のクライアント、およびそれを行うことができず、信頼されるエッジサーバからの暗号解読されたイベントを利用するさらなる５０のクライアントへの情報の配布を示す棒グラフ６００を含む。図3に関連して前に説明したとおり、セットのクライアント６１０ないし６２６が、暗号化されたイベントを、このイベントが時刻６５０にサーバによって送信された後の何からの時刻に受信する。次に、時刻６７０に、信頼されるエッジサーバが、暗号解読の鍵を配信することができる。したがって、図6で図示する例に示すとおり、暗号化されたイベントを記憶し、暗号解読する能力を有する１００のクライアントのすべてが、ほぼ同時刻に、すなわち、信頼されるエッジサーバが、時刻６７０に鍵を送信した2秒後にイベントに含まれる情報へのアクセスを受け取る。

【００５４】暗号化されたイベントを記憶し、暗号解読する能力を有さない残りの５０のクライアントに関しては、信頼されるエッジサーバが、そのイベントを暗号解読し、暗号解読されたイベントを時刻６８０に送信することができる。図6に図示する例では、時刻６８０は、暗号解読されたイベントを受信する最初のセットのクライアント６４０が、リリース時刻６６０より前には受信しないが、それでも、可能な限りリリース時刻６６０近くに暗号解読されたイベントを受信するように、信頼されるエッジサーバによって選択されている。さらなるセットのクライアント６４２、６４４、および６４６が、クライアントの信頼されるエッジサーバへの接続の待ち時間に応じて、リリース時刻６６０の後の何らかの時刻に暗号解読されたイベントを受信することができる。明らかなように、暗号化されたイベントを記憶し、暗号解読することができない５０のクライアントに関して、信頼されるエッジサーバが、それでも、暗号解読された鍵を使用することによってイベントを送信することによってそのイベントに記憶された情報へのアクセスを提供することができ、５０のクライアントのそれぞれが、リリース時刻６６０のすぐ後に、図3の元の１００のクライアントとともに暗号解読されたイベントを受信したので、比較的公正な方法でその提供を行うことができた。

【００５５】図6の信頼されるエッジサーバは、クライアントへの接続の待ち時間の推定を介して、暗号解読されたイベントの送信を開始する時刻６８０を決定することができる。当分野の技術者には周知のとおり、待ち時間は、データを転送する接続の能力の目安である。本発明は、信頼されるエッジサーバが、各クライアントまたは代表的セットのクライアントとの通信履歴を含むデータベースを保持できることを企図している。そのようなデータベースを使用して、経験的データに基づき、伝送の予期される時間を判定することができる。データベースは、データ転送速度、ピークデータ転送速度、輻輳情報、接続障害、ならびにクライアントとの前の通信から収集された他のそのようなネットワーク情報などの待ち時間の測定値を含むことが可能である。例えば、履歴上のデータ転送速度の平均値を使用してもよいし、またはデータ転送速度の最近の傾向を使用して、伝送に関する予期される時間の推定値を外挿することができる。替わりに、データ転送速度情報を追加の情報と併せて使用して、推定の伝送時間の導出を行う、または精度を高めることができる。経験的観測に基づく伝送の予期される時間に加え、信頼されるエッジサーバは、ネットワーキング機能を使用して伝送の理論上の時間を決定することができる。例えば、信頼されるエッジサーバは、クライアントまたはセットのクライアントに「ＰＩＮＧ」を行い、クライアントが応答するのにかかる時間を測定して、予期される伝送時間を判定することができる。替わりに、より進んだネットワーキング環境に、クライアントへの接続の待ち時間に関してさらなる情報を信頼されるエッジサーバに提供することができるより進んだネットワーキングプロトコルを持たせてもよい。

【００５６】リリース時刻から推定の伝送時間を引くことにより、信頼されるエッジサーバは、暗号解読されたイベントを受信するクライアントが、そのイベントをリリース時刻に受信できるようにする暗号解読されたイベントの送信を開始する送信時刻６８０を決定することができる。当分野の技術者には分かるとおり、推定の伝送時間は、イベントのサイズを接続の待ち時間で割ることによって判定することができる。

【００５７】ただし、接続の待ち時間は変化する可能性があるため、また一部の状況では、リリース時刻より前にイベントによって伝えられる情報にアクセスを得るクライアントが全く存在しないようにすることが極めて重要であるため、信頼されるエッジサーバは、伝送の最小の予期される時間を使用することによって送信時刻を決定し、これにより、最適の条件でも、暗号解読されたイベントが、リリース時刻より前にクライアントに着信しないのを確実にすることができる。伝送の最小の予期される時間は、データベースの中に記憶されている最低のデータ転送速度に基づくこと、または予期しないイベントを考慮に入れる適切な乗数を使用してネットワーク機能を介して獲得されたデータに基づくことが可能である。例えば、伝送の最小の予期される時間は、単に理論的計算を使用して導出された伝送の予期された時間の半分とすることが可能である。最小の予期の伝送時間を使用して、信頼されるエッジサーバは、リリース時刻より前にイベントに含まれる情報にアクセスを得るクライアントが存在しないようにするだけ十分に遅い送信時間を決定することができる。

【００５８】図７は、最低限の記憶能力または処理能力を有するクライアントに、イベントに含まれる情報へのアクセスを提供するため、本発明によって企図される別の可能性を示している。棒グラフ７００は、図６に関連して前述した棒グラフ６００と同様の状況を示している。ただし、図７では、信頼されるエッジサーバが、様々な時刻７８０ないし７８６に暗号解読されたイベントを送信し、暗号解読されたイベントを要求したクライアントのすべてが、ほぼ同時刻７４０にそのイベントを受信するようにすることができる。したがって、図６で最小の時間で暗号解読されたイベントを受信したセットのクライアント６４０に、信頼されるエッジサーバは、時刻７８６に暗号解読されたイベントの送信を開始することができる。次に高速のセットのクライアント６４２に、信頼されるエッジサーバは、時刻７８４に暗号解読されたイベントの送信を開始することができ、また同様に、信頼されるエッジサーバは、時刻７８２にクライアント６４４に、また時刻７８０にクライアント６４６にイベントの送信を開始することができる。個々のクライアントまたはグループのクライアントへの送信時刻を時差的にすることにより、信頼されるエッジサーバは、図７に示す時刻７４０にイベントを必要とするクライアントにほとんど同時刻にその暗号解読されたイベントを提供することができる。

【００５９】図７の信頼されるエッジサーバは、前述した経験的方法または理論的方法を介してクライアントまたはグループのクライアントとの間のおおよその接続待ち時間を判定することができ、またその推定値を使用して、様々なクライアントに暗号解読されたイベントを送信する時刻を決定することができる。さらに、信頼されるエッジサーバが、リリース時刻７６０より前に暗号解読されたイベントを送信することができる前に示した方法を使用して、信頼されるエッジサーバは、セット７４０の中のクライアントが、セット７３０の中のクライアントとほぼ同時刻にイベントに含まれる情報へのアクセスを得るようにすることもできる。

【００６０】図２に戻ると、ネットワーク接続２-１８および２２８が、直接接続として示されているが、当分野の技術者には明らかとなるとおり、そのような接続は、任意の数のルータ、信頼されるサーバ、信頼されないサーバ、および他のネットワークパスを含むことが可能である。本発明は、信頼されるサーバ、および以下に述べられるエッジサーバへの接続が、必ずしも特定のハードウェア構成または何らかの物理的限定を必要とせず、既存のハードウェア上で実行されるソフトウェアで実施できることで、オーバーレイネットワークを企図している。この結果、以下にさらに詳細を述べる図２のネットワーク２００は、単に既存の物理的ネットワーク上のソフトウェアオーバーレイを表すこと、または新しいネットワークの物理構造を表すことが可能である。

【００６１】図２に示す信頼されるエッジサーバへの接続２１８は、中間の信頼されないサーバを含むことが可能である。以下により詳細に説明するとおり、リリース時刻より前に起点のサーバ２１０からネットワーク２００全体に暗号化されたイベントが送信される。イベントは、暗号化されているため、イベント配信の完全性を危うくすることなく、接続パス２１８における信頼されないサーバを介して信頼されるエッジサーバまで送られることが可能である。ただし、リリース時刻より前に信頼されるエッジサーバ２２０、２２１および２２２に暗号解読の鍵が提供される場合は、保護対策を使用して、サーバから、または接続パス２１８における信頼されないサーバが、リリース時刻より前に鍵を獲得してクライアントに配信しないようにすることを確実にすることができる。本発明で使用することができる保護対策の例には、当技術分野で周知の仮想プライベートネットワーキング（ＶＰＮ）およびポイントツーポイントトンネル伝送プロトコル（ＰＰＴＰ）を可能にする暗号化アルゴリズムが含まれる。そのようにすると、起点のサーバ２１０は、以下に詳細に説明するとおり、接続パス２１８における信頼されないサーバにセンシティブな情報を同時に明かすことなく、信頼されるエッジサーバに暗号解読の鍵、および暗号解

読されたイベントまたは暗号化されていないイベントを含め、センシティブな情報をセキュアに通信することができる。

【0062】図2のネットワーク200は、ブロードバンドのクライアント150が接続されているものとして信頼されるエッジサーバ222を示している。したがって、信頼されるエッジサーバ222が、図3に示すように、リリース時刻より前に暗号化されたイベントを提供することができ、またブロードバンドのクライアントが、そのイベントを記憶し、暗号解読する能力を有する可能性が高い。ただし、ナローバンドのクライアント50だけが接続されているものとして示される信頼されるエッジサーバ220が、図4に示すように、ナローバンドのクライアント50のそれぞれが、暗号化されたイベントをリリース時刻より前に受信しているようにするだけ十分に早い送信時刻に暗号化されたイベントを送信しないようにすることが可能である。そのようなネットワーク状況を所与として、本発明は、暗号解読の鍵の発行を調整するように信頼されるエッジサーバ222と220の間、または信頼されるエッジサーバ220、221、222、および起点のサーバ210のすべての間の通信を企図している。図4に関連して前述したとおり、信頼されるエッジサーバは、リリース時刻460の後、終了時刻490までの任意の時刻に暗号解読の鍵を伝送することができる。したがって、470の鍵送信時刻は、他の信頼されるエッジサーバの鍵送信時刻に一致させることが可能である。したがって、信頼されるエッジサーバ222は、図3に示すように、リリース時刻より前に暗号化されたイベントを既に配信していても、図4に示すとおり、リリース時刻の後である鍵送信時刻470に一致するように鍵送信時刻370を遅延させることが可能である。

【0063】調整メッセージ等を信頼されるエッジサーバ間で、または信頼されるエッジサーバと起点のサーバの間で送信して鍵の伝送を調整することができる。替わりに、この調整が、前述した中央鍵サーバによって行われることが可能である。中央鍵サーバは、クライアントが暗号化されたイベントを受信している程度を示す信頼されるエッジサーバからの、またはクライアント自体からのメッセージを受信することができる。その情報に基づき、中央鍵サーバは、調整された鍵送信時刻を決定し、その調整された鍵送信時刻に鍵をクライアントに送信すること、あるいは調整された鍵送信時刻の直前に鍵を送信することによるか、または調整された鍵送信時刻に鍵を送信するように信頼されるエッジサーバに命令を提供することにより、クライアントに転送するよう、信頼されるエッジサーバに鍵を送信することができる。さらに、それぞれの信頼されるエッジサーバおよび起点のサーバの時刻設定を調整するメッセージも送信して、時刻の不適切な設定によりタイミングが悪い鍵の伝送が生じるのを防止することができる。また、中央鍵サーバ、または鍵サーバのネットワークも、信頼されるエッジサーバに合わせて自らの時刻を調整することができる。サーバのすべての時刻設定、つまりクロックを調整するための1つの方法は、ネットワーク時刻プロトコルを使用して、政府の標準設定機関によって提供されるような標準時刻にサーバを同期させることである。フェールセーフとして、各信頼されるエッジサーバが、調整メッセージを受信しなかった場合、リリース時刻が過ぎているという条件付きで、自らのクライアントがレディーになるとすぐに鍵を送信することができる。

【0064】また、本発明は、信頼されるエッジサーバ[illegible]ことができるとが、イベントを暗号解読し、暗号解読されたイベントを[illegible]伝送しなければならないときでさえ、信頼されるエッジ[illegible]サーバ、特殊化された中央鍵サーバ、特殊化された分散[illegible]鍵サーバ、起点のサーバ、または以上のサーバの組み合[illegible]わせの間の鍵送信時刻調整を企図している。例えば、前述した図2のネットワーク環境に戻ると、信頼されるエッジサーバ221に、前述した図6または7に示したような方法で信頼されるエッジサーバ221がイベントを[illegible]暗号解読し、暗号解読されたイベントを伝送するのを必要とするが、[illegible]要とするクライアントが接続されていることが可能である。図6および7に示すとおり、信頼される[illegible]、起点のサーバは、時刻680に、または一連の時刻780、782、784、および786に暗号解読されたイベントの各クライアントまたは送信を開始することができる。さらに、前述したとおり、サーバに[illegible]のコピーをとり、送信時刻は、信頼されるエッジサーバとクライアント、ブロードキャストの間の接続の推定された待ち時間に基づいて計算することができる。ただし、前述した計算は、一般に、リリース時刻に暗号解読されたイベントへのアクセスを提供する。信頼されるエッジサーバまたは起点のサーバが、リリース時刻より後の時刻に鍵を送信するように調整している場合、暗号解読されたイベントを送信する信頼されるエッジサーバは、計算においてリリース時刻の代わりにその調整された時刻を使用して暗号解読されたイベントの送信時刻を決定することができる。そのようにすると、暗号解読されたイベントを受信するクライアントは、暗号化されたイベントを受信しており、鍵を待っているクライアントより前にイベントに含まれる情報にアクセスを受けることがない。

【0065】信頼されるエッジサーバ間で鍵および暗号解読されたデータの伝送の調整を行うための1つの方法は、起点のサーバ210のような起点のサーバから信頼されるエッジサーバにイベントが配信される受信時刻に基づくことが可能である。信頼されるエッジサーバが、起点のサーバから十分に早期にイベントを受信しなかった場合、クライアントへの暗号化されたイベントの伝送は、図4に示した状況のようにリリース時刻より前に完了しない可能性がある。しかし、前述したような経験的推定または理論的推定を介して、信頼されるエッジサー

バは、自らのクライアントへの接続の推定の伝送時間を獲得することができ、これにより、クライアントのすべて、または大多数への暗号化されたイベントの伝送を完了するのに要する伝送時間を推定することができる。次に、暗号化されたイベントの伝送が完了するが、それでも終了時刻より前であるその推定時刻より後になるよう、暗号解読の鍵を送信するための調整された時刻を選択することができる。調整された時刻が選択されると、暗号解読されたイベントを送信する信頼されるエッジサーバは、より詳細に前述した方法で、リリース時刻ではなくその時刻を使用して、暗号解読されたイベントをいつ送信するかを決定することができる。

【００６６】本発明は、暗号化されたイベント、暗号解読されたイベント、および暗号解読の鍵を含め、ネットワーク環境２００全体でデータを伝送するための効率的なネットワークプロトコルの使用を企図している。１つのそのようなプロトコルが、インターネットプロトコル（ＩＰ）を使用するネットワークで一般的なマルチキャスティングプロトコルである。当分野の技術者には分かるとおり、マルチキャストトラフィックは、単一の宛先ＩＰアドレスに送信されるが、複数のＩＰホストにより、ネットワーク環境２００におけるＩＰホストの場所に関わらず受信され、処理される。トラフィックは、単一の宛先ＩＰアドレスに送信されるため、マルチキャスティングにより、各クライアントまたはそれぞれの信頼されるエッジサーバに個別のコピーを送信する必要性が回避される。ただし、ブロードキャストとは異なり、マルチキャスティングは、特定のＩＰマルチキャストアドレスを聴取しているネットワークデバイスだけが、情報を受信し、処理するのを可能にする。一般に、ホストグループは、所定のＩＰマルチキャストアドレスで聴取を行っているホストのセットとして定義される。ホストグループのサイズに制限は存在せず、またホストグループのメンバシップが変化すること、また別の方法で動的とすることが可能である。さらに、ホストグループは、いくつかのルータおよび複数のネットワークセグメントにまたがっていることが可能であり、情報を指定のＩＰマルチキャストアドレスにマルチキャストするのに、計算デバイスが、ホストグループのメンバであることは必要とされない。アプリケーションは、マルチキャストを受信するのに、自らが所定のＩＰマルチキャストアドレスでマルチキャストを受信することを適切なネットワーキング層に知らせることができる。

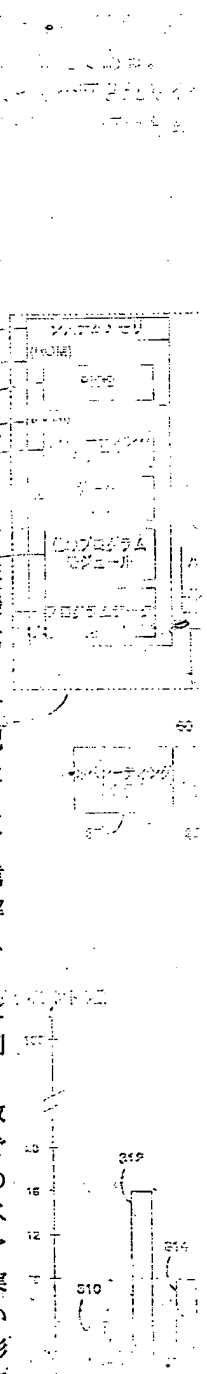
【００６７】ただし、マルチキャスティングの性質のため、タイミングが重要である状況では、ホストのすべてが、再送を要求する必要なしに伝送されたデータを受信することが好ましい。データが適切に受信される確率を高めるための１つの方法は、冗長性、または他の誤り訂正アルゴリズムを使用することである。暗号解読の鍵などのデータの小さい要素の場合、冗長性が最も簡単な解決策である。例えば、暗号解読の鍵は、数キロバイトまたはそれより小さいオーダのものとすることが可能である。１０倍の冗長性が実施されたとしても、メッセージのサイズが、増加するのはおよそ３０キロバイトまでである。５６ｋｂｐｓで、さらには３３．６ｋｂｐｓで動作する従来のアナログモデムなどのナローバンド接続を使用してさえ、３０キロバイトをダウンロードするのに、１０秒間ほどしかかからない可能性がある。したがって、従来の標準で、相当な量の冗長性を使用することによってさえ、短い時間幅の中で暗号解読の鍵の伝送を達することができる。

【００６８】鍵のサイズが小さいことにより、複数のサーバが、ネットワークの待ち時間にそれほど影響を与えることなく、ネットワーク２００全体に鍵を伝送することが可能になる。鍵を伝送するのに複数のサーバを利用することにより、複数のネットワークパスを使用してクライアントのそれぞれに鍵を配信することができる。各クライアントが、複数のネットワークパスを介して鍵を受信することができるため、輻輳の生じたノード、またはその他のネットワークボトルネックにより、クライアントのそれぞれへの鍵の伝送時間が影響を受ける可能性が相当に低くなる。というのは、クライアントが、輻輳の生じていないパスを介して少なくとも１つの鍵を受信する可能性が高いからである。

【００６９】明らかなように、本発明は、信頼されるサーバに接続されたクライアントへのイベントの公正な配信を、クライアントの帯域幅の違いにも関わらず可能にする。信頼されるエッジサーバが、イベントを暗号化し、伝送される鍵を介してリリース時刻に、または終了時刻より前に暗号解読されるようにクライアントに配信するか、またはリリース時刻より前にイベントの暗号解読されたバージョンを伝送するのを開始して、リリース時刻に、または終了時刻より前にそのイベントがクライアントに着信するようにすることができる。そのようにすると、可能な限り多くのクライアントに、ほぼ同時刻にイベントへのアクセスが提供される。

【００７０】本発明の原理を適用することができる多数の可能な実施形態に鑑みて、図面に関連して本明細書で説明した実施形態は、例示することだけを意図するものであり、本発明の範囲を限定するものと受け取られるべきではないことを認識されたい。例えば、ソフトウェアで示した例としての実施形態の要素をハードウェアで実装するのが可能であり、またその逆も真であり、あるいは本発明の趣旨を逸脱することなく、例としての実施形態の構成および詳細を変更できることが、当分野の技術者には認められよう。したがって、本明細書で説明した本発明は、頭記の特許請求の範囲および等価のものに含まれることが可能なすべてのそのような実施形態を企図している。

【図面の簡単な説明】



39

【図１】本発明が存在する例としてのコンピュータサーバを一般的に示すブロック図である。

【図２】本発明が機能することが可能な例としてのネットワーク環境を一般的に示すブロック図である。

【図３】本発明によって企図されるイベントを配信する方法を一般的に示す時間図である。

【図４】本発明によって企図されるイベントを配信する方法を一般的に示す別の時間図である。

【図５】本発明によって企図されるイベントを配信する方法を一般的に示す別の時間図である。

40

【図６】本発明によって企図されるイベントを配信する方法を一般的に示す別の時間図である。

【図７】本発明によって企図されるイベントを配信する方法を一般的に示す別の時間図である。

【符号の説明】

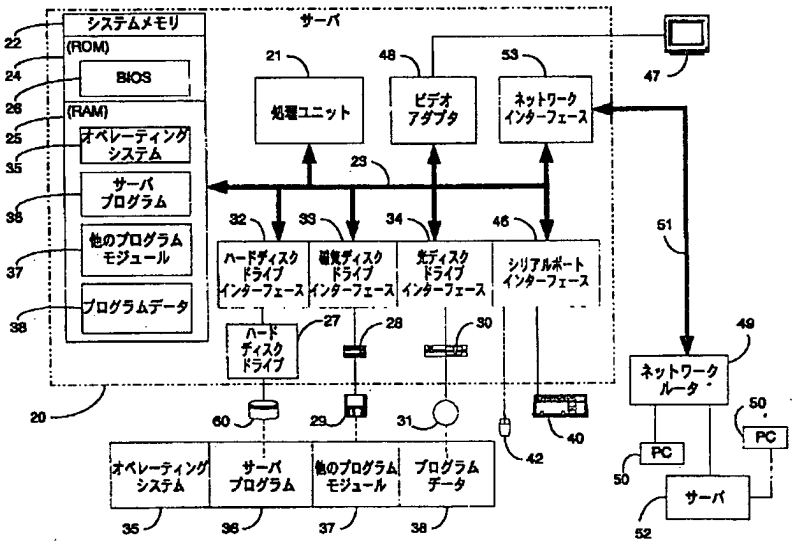
５０、１５０　クライアント

２００　ネットワーク環境

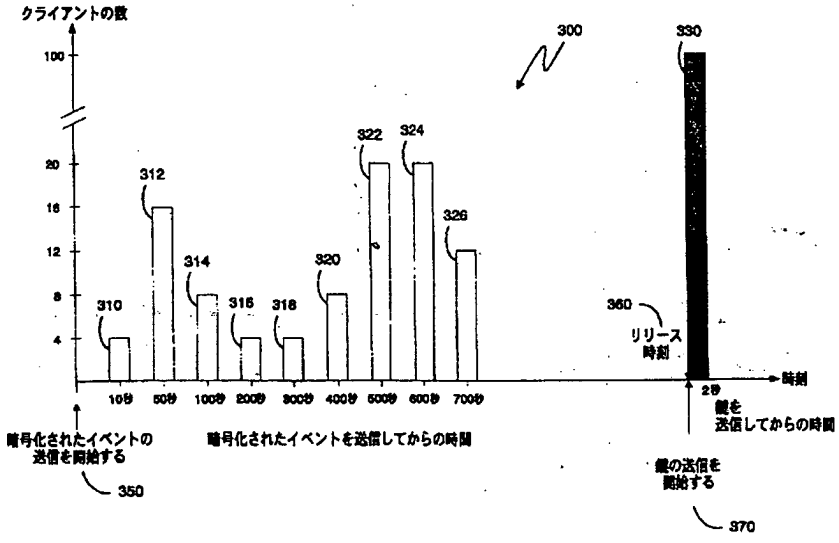
２１０、２２０、２２１、２２２、２３０、２３１、２３２　サーバ

２１８、２２８、２３８、２３９　接続

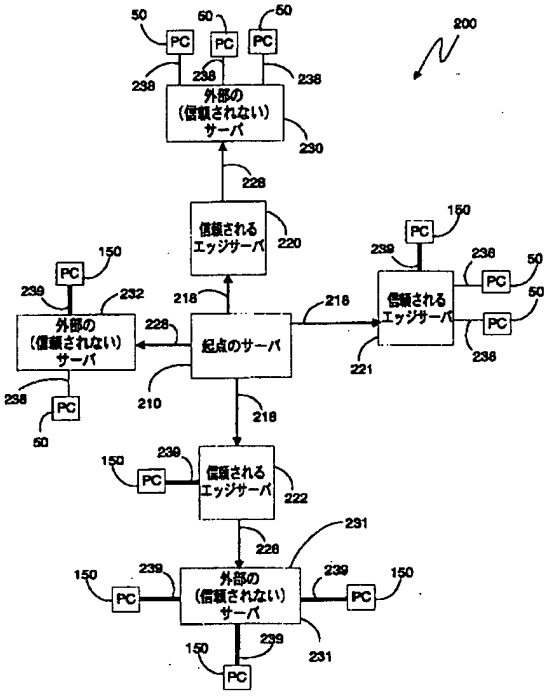
【図1】



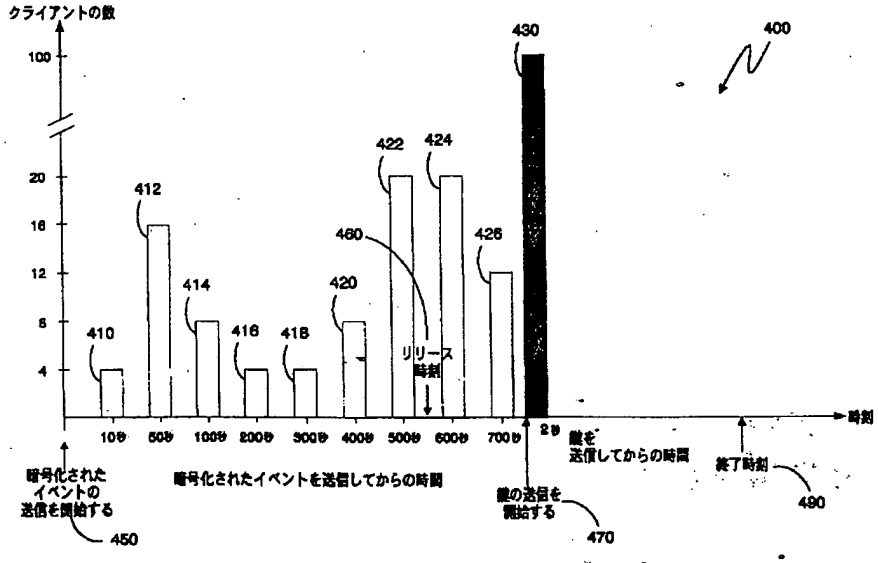
【図3】



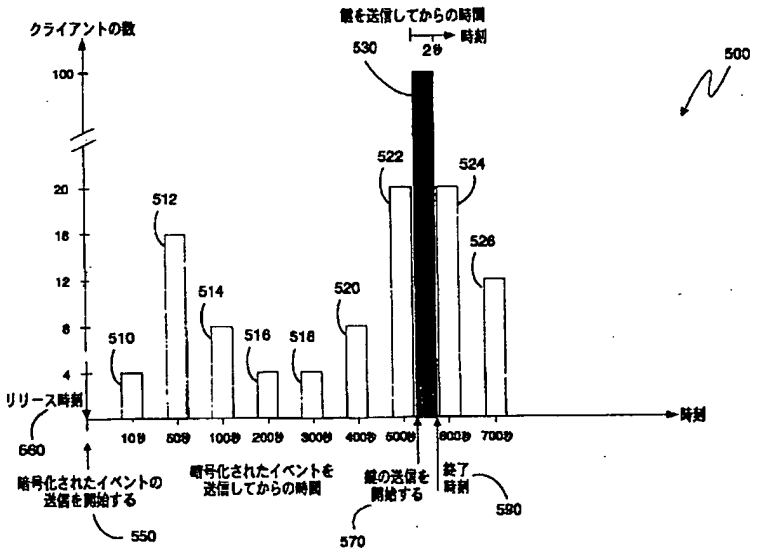
【図2】


200
PC
50
238
236
外部の
(信頼されない)
サーバ
230
228
信頼される
エッジサーバ
220
150
239
232
218
外部の
(信頼されない)
サーバ
起点のサーバ
210
信頼される
エッジサーバ
221
信頼される
エッジサーバ
222
231

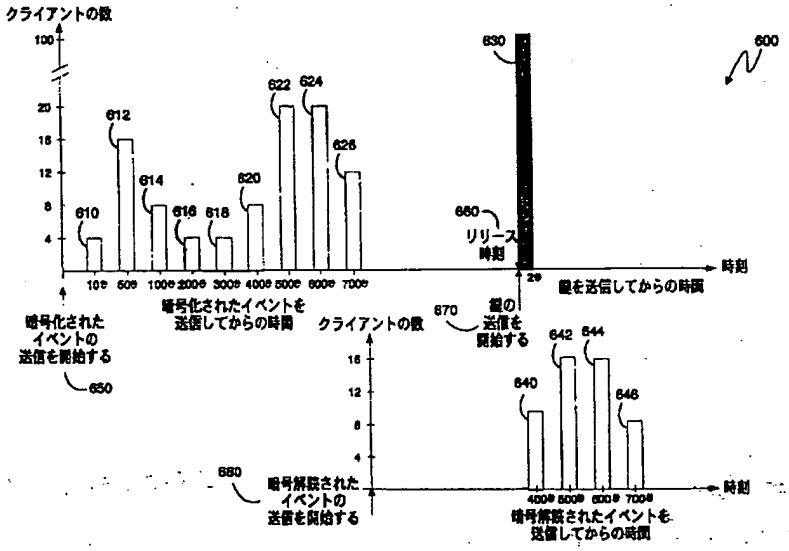
【図4】


クライアントの数
100
20
16
12
8
4
400
430
422
424
412
460
426
414
420
410
416
418
リリース
時刻
時刻
10秒
50秒
100秒
200秒
300秒
400秒
500秒
600秒
700秒
2秒
鍵を
送信してからの時間
終了時刻
490
暗号化された
イベントの
送信を開始する
450
暗号化されたイベントを送信してからの時間
鍵の送信を
開始する
470

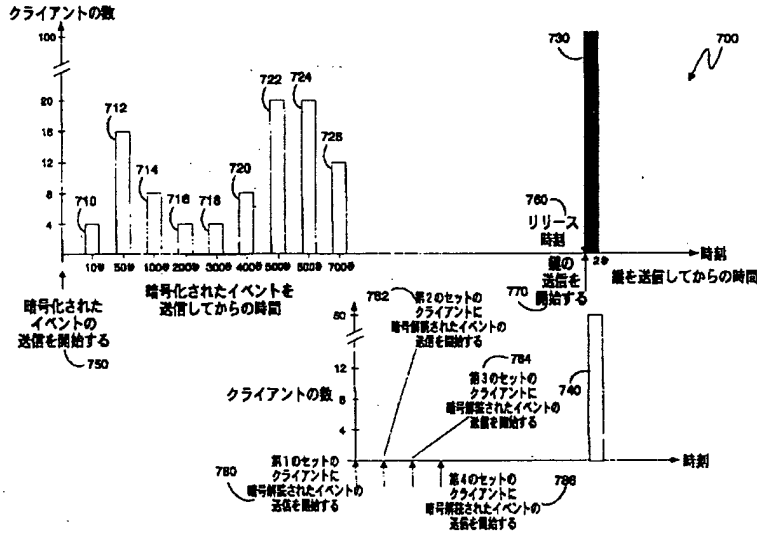
【図5】


クライアントの数
鍵を送信してからの時間
時刻
530
500
522
524
512
526
514
520
510
516
518
リリース時刻
560
時刻
暗号化されたイベントの送信を開始する
550
暗号化されたイベントを送信してからの時間
鍵の送信を開始する
570
終了時刻
590

【図6】


クライアントの数
600
630
612
622
624
614
626
610
620
616
618
660
リリース時刻
時刻
暗号化されたイベントの送信を開始する
650
暗号化されたイベントを送信してからの時間
鍵を送信してからの時間
670
鍵の送信を開始する
クライアントの数
642
644
640
646
680
暗号解読されたイベントの送信を開始する
時刻
暗号解読されたイベントを送信してからの時間

【図7】



フロントページの続き

(72)発明者　ベンカタ　エヌ．パッドマナブハン
アメリカ合衆国　98007　ワシントン州　ベルビュー　146　プレイス　ノースイースト　3620　アパートメント　ディー－３

(72)発明者　ルイス　フェリペ　カブレラ
アメリカ合衆国　98004　ワシントン州　ベルビュー　キラーニー　ウェイ　サウスイースト　2009

Ｆターム(参考)　5B085 AA08 AE29
5J104 AA16 BA03 EA04 EA15 EA16 NA02 PA07